PostHog

SOC 2 Type 2

Report on the Description of the Analytics Platform and on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality for the Period June 1, 2025 to May 31, 2026

and Independent Service Auditor's Report Thereon

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

www.schneiderdowns.com

TABLE OF CONTENTS

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

SECTION I: INDEPENDENT SERVICE AUDITOR'S REPORT

PostHog, Inc.
San Francisco, California

SCOPE

We have examined PostHog, Inc.'s (PostHog) accompanying description of its Analytics Platform found in Section III titled "Description of PostHog, Inc.'s Analytics Platform" throughout the period June 1, 2025 to May 31, 2026 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 1, 2025 to May 31, 2026, to provide reasonable assurance that PostHog'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 (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

PostHog uses a subservice organization to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at PostHog, to achieve PostHog's service commitments and system requirements based on the applicable trust services criteria. The description presents PostHog's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of PostHog's controls. The description does 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 description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at PostHog, to achieve PostHog's service commitments and system requirements based on the applicable trust services criteria. The description presents PostHog's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of PostHog'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.

The information in Section V titled "Other Information Provided by PostHog, Inc." is presented by PostHog's management to provide additional information and is not a part of PostHog's description of its Analytics Platform made available to user entities during the period June 1, 2025 to May 31, 2026. Information about PostHog's management responses to the auditor's exceptions has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

SERVICE ORGANIZATION'S RESPONSIBILITIES

PostHog 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 PostHog's service commitments and system requirements were achieved. In Section II, PostHog has provided the accompanying assertion titled "Management Assertion of PostHog, Inc." (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. PostHog is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

SERVICE AUDITOR'S RESPONSIBILITIES

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves—

- 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

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. 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 are 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.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section IV of this report.

Opinion

In our opinion, in all material respects—

1. the description presents PostHog's Analytics Platform that was designed and implemented throughout the period June 1, 2025 to May 31, 2026 in accordance with the description criteria.
2. the controls stated in the description were suitably designed throughout the period June 1, 2025 to May 31, 2026 to provide reasonable assurance that PostHog's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of PostHog's controls throughout that period.
3. the controls stated in the description operated effectively throughout the period June 1, 2025 to May 31, 2026 to provide reasonable assurance that PostHog's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization and user entity controls assumed in the design of PostHog's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of PostHog; user entities of PostHog's Analytics Platform during some or all of the period June 1, 2025 to May 31, 2026; business partners of PostHog subject to risks arising from interactions with the Analytics Platform; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.

- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Schneider Downs & Co., Inc.

Pittsburgh, Pennsylvania
August 3, 2026

SECTION II: MANAGEMENT ASSERTION OF POSTHOG, INC.

We have prepared the accompanying description of PostHog, Inc.'s (PostHog) Analytics Platform titled "Description of PostHog, Inc.'s Analytics Platform" throughout the period June 1, 2025 to May 31, 2026 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria). The description is intended to provide report users with information about the Analytics Platform that may be useful when assessing the risks arising from interactions with PostHog's system, particularly information about system controls that PostHog has designed, implemented, and operated to provide reasonable assurance that its 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 (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

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

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

We confirm, to the best of our knowledge and belief, that—

1) the description presents PostHog's Analytics Platform that was designed and implemented throughout the period June 1, 2025 to May 31, 2026 in accordance with the description criteria.

2) the controls stated in the description were suitably designed throughout the period June 1, 2025 to May 31, 2026 to provide reasonable assurance that PostHog's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of PostHog's controls throughout that period.

3) the controls stated in the description operated effectively throughout the period June 1, 2025 to May 31, 2026 to provide reasonable assurance that PostHog's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization and user entity controls assumed in the design of PostHog's controls operated effectively throughout that period.

Signed by:
Fraser Hopper
F559B6A059D6472...
Fraser Hopper, Operations and Finance Lead

August 3, 2026
Date

SECTION III: DESCRIPTION OF POSTHOG INC.'S ANALYTICS PLATFORM

BACKGROUND AND OVERVIEW

PostHog Inc. ("PostHog" or the "Company") provides a suite of analytics tools that allows companies to better understand how users interact with their products. The Company was founded in 2019 and is based in San Francisco, California. The PostHog Analytics Platform features the following tools and products:

- Product Analytics
- Web Analytics
- Session Replay and Recordings
- Feature Flags
- A/B Testing and Experiments
- Event and Data Pipelines
- Data Warehouse
- Error Tracking
- Heatmaps
- Surveys
- LLM Analytics (AI Observability)
- PostHog AI

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Principal Service Commitments

PostHog designs its processes and procedures related to the PostHog Analytics Platform to meet its objectives. Those objectives are based on the service commitments PostHog makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational and compliance requirements that PostHog has established for the services. System services are subject to the security, availability, and confidentiality requirements of the SOC 2 framework, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which PostHog operates.

PostHog makes the following security, availability, and confidentiality commitments to its customers:

- Customer data is always encrypted at rest and in transit.
- Use of intrusion prevention systems (IPS) to prevent and identify potential security attacks from users outside the boundaries of the system.
- The platform is continuously monitored and tested for any security vulnerabilities or unexpected changes.
- PostHog requires employees to undergo a background check, acknowledge a Confidential Information and Invention Assignment Agreement or similar intellectual property and confidentiality agreement upon hire, acknowledge an Acceptable Use Policy and complete security awareness training on an annual basis.

- Disaster recovery plans are in place and tested at least once per year.
- System features and configuration settings are designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Databases are located in private subnets and are not exposed to the public.
- Processing capacity and usage are monitored to appropriately manage capacity demand and to enable the implementation of additional capacity to meet availability commitments.
- Confidential Information and Invention Assignment Agreements or similar intellectual property and confidentiality agreements are executed with all employees and third parties with access to confidential customer information.

System Requirements

PostHog establishes operational requirements that support the achievement of security, availability, and confidentiality commitments, relevant laws and regulations and other system requirements. Such requirements are communicated in the Company'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. Standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the system.

COMPONENTS OF THE SYSTEM

Boundaries of the System

The System subject to this SOC 2 examination consists of the infrastructure, software, people, procedures, and data used by PostHog to provide the Analytics Platform services to user entities, as described in this report.

The following are expressly outside the boundaries of the System described in this report:

- The Company's internal financial reporting systems and processes are outside the scope of this examination.
- The Company's human resources information system (HRIS), used solely for payroll and benefits administration, is outside the scope of this examination.
- Data provided by user entities that exists solely on user entity systems prior to transmission to the System is outside the Company's system boundaries.

Infrastructure

PostHog runs in Amazon Web Service (AWS), utilizing the Elastic Kubernetes Service (EKS), Kafka and Aurora Databases.

Each platform instance (production, development, test) is contained within a separate AWS account. This approach provides granular access control to all aspects of the infrastructure. Access from external locations is controlled through configuration and firewall rules. Access to internal components of the platform is only possible via multifactor authentication (MFA) controlled access utilizing Secure Shell (SSH) protocol. Access is granted on an environment and component within each account (i.e., pods, storage and database) basis.

Data is persisted via AWS Aurora Postgres Services utilizing Advanced Encryption Standard (AES) 256 encrypted disks for all data stored at rest.

User entities access their instance using standard web browsers utilizing Transport Layer Security (TLS) 1.2 or above for encrypted communications.

Software

PostHog is a web-based Software-as-a-Service (SaaS) application and uses AWS EKS as a Platform-as-a-Service (PaaS) solution. Kubernetes enables software deployments via images, which are secure, fully contained versions of the platform service. PostHog has several services that provide scalable system operations. Image-operating environments are based on a secure version of the Debian Linux distribution. PostHog's services are primarily developed using JavaScript and Python-based technologies.

Customers provide data to PostHog as described above via the web portal. Data is stored in AWS Managed Streaming for Apache Kafka and processed by the Company's consumer services. The output of the consumers is stored in AWS Aurora.

The following applications, tools and services are also utilized by PostHog as part of its services and internal control environment:

Primary Infrastructure and Software	
System / Application	**Business Function / Description**
GitHub	Source code repositories, version control systems, build software and reviews
AWS CloudFront	Provides a Content Delivery Network (CDN) to increase security and bring data closer to where the customer is located
AWS Managed Streaming for Apache Kafka	Message queue system
Cloudflare	Denial-of-Service (DNS) services and web application firewall (WAF), including distributed DNS attack protection; PostHog requires Secure Socket Layer (SSL) on all public-facing web services and uses Cloudflare to create and manage those SSL certificates
Wiz	Cloud infrastructure monitoring
1Password	Internal password vault
Google Suite	Internal identity management system
Slack	Internal communications system

People

PostHog has a staff of approximately 206 employees organized into small teams, that broadly fall into the following functional areas:

- **Executive Management** – responsible for overseeing operations of the Company
- **Infrastructure & Engineering** – develop, innovate and support the technology
- **Product Management** – support PostHog product management, development and development operations
- **Customer Success** – work with customers to ensure they're able to successfully use PostHog to accomplish their goals and work to convert app users into paying customers

- **People & Operations** – support back-office operations
- **Information Security** – responsible for maintaining the Information Security Program and controls within the Company.

Processes and Procedures

Management has developed and communicated processes that control and restrict access to the PostHog app instances that contain customer data. Changes to these procedures are performed annually and authorized by senior management. They cover the following key security lifecycle areas:

- Data classification (data at rest, in motion, 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 (e.g., firewalls).

Data

Information assets are assigned a sensitivity level based on the audience for the information. If the information has been previously classified by regulatory, legal, contractual or company directive, that classification takes precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data is assigned to one of the following security levels:

- **Confidential Data**: Highly valuable and sensitive information where the level of protection is dictated internally. If this information is exposed in some way, it would be damaging for PostHog and the Company's reputation. Access to confidential data is limited to authorized employees, contractors and business partners.
- **Internal Data**: No one outside of PostHog should have access to internal data on anything PostHog owns or licenses. The Company restricts access to those employees who need to know the information, but it is information that might not have a legal requirement to be kept secure.
- **Public Information**: Any information PostHog has that the public can access. The Company is not legally required to keep this information secure but nonetheless does so.

Example Data	Classification	Description of Data	Data Store
Customer data	Confidential	PostHog stores information that customers enter into the platform, such as clients of the customers.	AWS Aurora
Usage information	Internal Use	PostHog keeps track of user activity in relation to the types of services customers and their users use, and performance metrics related to their use of the services.	AWS Aurora
Log information	Internal Use	PostHog collects platform logs and information about customers and their users, including Internet Protocol (IP) addresses. Log files are immutable records of computer events or user activity that form an audit trail. These records may be used to assist in detecting security violations, performance problems and flaws in applications.	EBS (Elastic Block Store)

Customer data is retained in accordance with customer agreements and legal, privacy or regulatory obligations. Customers can request that their data is deleted and have the ability to self-serve such deletion via the Analytics Platform interface. If PostHog is able to do that while complying with legal or regulatory obligations, it will complete such requests within 30 days.

System Incidents

During the period June 1, 2025 to May 31, 2026, the Company did not identify any system incidents that resulted from controls that were not suitably designed or operating effectively, or that resulted in a significant failure in the achievement of the Company's service commitments or system requirements.[

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring of Controls

Control Environment

Management Philosophy

PostHog's control environment reflects the philosophy of senior management concerning the importance of the security of analytics data and information. The Chief Technology Officer (CTO) reports to the board annually and is charged with establishing overall security policies and procedures. The importance of security is emphasized within PostHog through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. In designing its controls, PostHog has taken into consideration the relevance of controls to meet the relevant trust services criteria.

Security Management

Security at PostHog is managed by the Executive Management, Infrastructure & Engineering, Information Security and People & Operations teams who are responsible for developing, maintaining and enforcing PostHog's information security policies. The information security policy is reviewed and approved annually by the CTO.

As PostHog maintains security, it monitors known incidents and patches, as well as results from recent vulnerability assessments, and addresses necessary changes to policies and procedures. Changes can include reclassification of data, reassessment of risk, changes in incident response plans and verification of responsibilities for authorizing and monitoring access.

Management ensures communication of the latest security policies to all employees during annual security training and awareness programs.

Security Policies

PostHog has defined a set of information security standards and policies that are under the direction and ownership of the Executive team. Standards and policies address the management and implementation of security controls, ranging from the physical security of facilities and equipment to the logical security at the data element layer. Information security policies and standards are designed to provide information to employees, contractors and vendors that is aligned to their job or functional responsibilities while also contemplating segregation of functions that may otherwise create a segregation of duties conflict.

Security policies are published on Drata, PostHog's controls monitoring platform, included in onboarding packages and reiterated through annual training that all employees are required to take and acknowledge.

All employees are required to review the Code of Conduct and all other company policies at the time of hiring. Confidentiality, computer security, general expectation of business behavior, performance and financial dealings are addressed within the policies. Employees must avoid any appearance of impropriety or conflict of interest. It is a policy that no employee shall engage in any outside activity that interferes with his or her job, competes with PostHog's activities or involves any use of PostHog's equipment. Employees are required to sign a Confidential Information and Invention Assignment Agreement or similar intellectual property and confidentiality agreement upon hire.

Personnel Security

Background checks are performed on all new hires as a condition of employment, who are also required to review and acknowledge their receipt of relevant security policies. New positions are supported by job descriptions. Once engaged, personnel are subject to PostHog procedures for accessing systems. Employees who violate PostHog's information security policy are subject to related disciplinary action. Employees are instructed to report potential security incidents to the CTO and to PostHog's Security team.

Physical Security and Environmental Controls

All PostHog centralized data storages are housed by the Company's PaaS and IaaS provider that have annual SOC 2 Type 2 examinations and provide controls for physical security and environmental controls.

No servers or computer facilities for the PostHog applications are hosted onsite. All computer facilities and access thereto are controlled at the cloud infrastructure datacenters.

Change Management

The change management process has been established to plan, schedule, approve, distribute and track changes to the production environment through designated responsibilities, with the objective of minimizing risk and customer impact. It further controls the integrity and reliability of the environment while maintaining the pace of change required for business purposes. The full process is documented within the Change Management Policy.

Proposed changes are managed through a formal change and release management procedure and tracked using a centralized ticketing system. The categorization of these changes is based on priority and risk associated with the change. Changes are requested, approved, tracked and implemented throughout the release lifecycle, which includes product and engineering planning, release management, deployment and post-deployment support phases. Change requests are documented, assessed for their risk and evaluated/approved by the designated personnel.

All changes are tested in a separate test environment prior to migration. PostHog's software development process includes several steps that incorporate security and quality review, including code review, automated static code analysis checks on each change request, weekly security vulnerability testing and annual third-party penetration and security tests. Once deployed, changes are monitored for success; failed implementations are immediately rolled back, and the change is not considered completed until it is implemented and validated to operate as needed.

Patch Management

PostHog runs on AWS Kubernetes service, whose operating system has periodic releases that address issues, add functionality and resolve security issues. AWS notifies PostHog of new releases and PostHog Infrastructure & Engineering team monitors and manages patches accordingly. Security patches are primarily applied automatically when AWS recycles EKS worker nodes, which happens regularly as part of infrastructure maintenance. Additionally, AWS-managed services such as Managed Streaming for Apache Kafka (MSK) apply security patches automatically. Where applicable, patches are first deployed to test environments and monitored. In the event of zero-day or high-severity security issues, patch application and node recycling are accelerated to ensure timely deployment across all PostHog instances.

This process is accelerated in the event of a zero-day or high-severity security issue. High-severity security issues are tested for one day. Provided the patch passes, it is then applied to all other PostHog instances.

Firewalls and Perimeter Security

All PostHog instances are deployed in AWS, which provides firewall and perimeter security. Default configuration in all AWS instances is to restrict all traffic. Only the ports and protocols necessary to run the platform are enabled. Only PostHog Infrastructure & Engineering team has access to the AWS firewall settings, which are reviewed quarterly to ensure that all settings continue to meet platform requirements. PostHog also runs weekly vulnerability scans and annual penetration tests on the production instances, which report on any changes to perimeter security.

AWS provides multiple redundant layers to the network and firewall, along with native intrusion and prevention services which include the use of GuardDuty.

Data Backup and Recovery

PostHog has multiple redundant backup strategies in place for its production environment. All customer data is hosted on production-grade PostgreSQL instances managed by AWS Aurora, with continuous protection enabled. Every write to any of PostHog's production databases is automatically replicated to storage in multiple datacenters. Databases are configured for high availability and automatic failover, so in case any instance becomes unavailable, it is

automatically replaced with a standby. PostHog also performs automated logical backups of its production databases daily. Weekly backups are stored for eight weeks and monthly backups for 12 months. Backup files are periodically tested to ensure integrity.

Disaster Recovery and Business Continuity

PostHog's business continuity and disaster recovery plans help ensure recoverability and contingency from significant business disruption. Both focus on ensuring the Company's critical business functions and technologies will continue to operate despite any significant disruption that might otherwise have caused an interruption or will be recovered to an operational state.

These plans are reviewed and updated on at least an annual basis. Revisions to infrastructure and procedures in many cases require updates to occur more frequently. Testing of the plans include but is not limited to tabletop exercises, backup restores and annual rehearsals of the plan if an actual scenario did not occur. Results of tests and issues and mitigation plans are recorded post-test. PostHog has a recovery time objective (RTO) and recovery point objective (RPO) of six hours.

PostHog completes an annual risk assessment. As part of this process, any risks to business continuity are discussed and mitigation plans are developed for those that have a moderate to high risk of occurrence. Mitigation plans include adjusting operating procedures to ensure critical business functions are maintained throughout any incident period.

System Account Management

Controls are in place to prevent unauthorized access by PostHog personnel. PostHog's System Access Control Policy establishes the requirements for requesting and provisioning user access to the system. Where possible, PostHog uses a centralized authentication and authorization system to restrict access to other systems and services within the environment. Each user account is unique and identifiable to an individual user.

MFA for access to core systems is enforced by Okta and Google Workspace, requiring users to have two factors to authenticate access to the system, one being a password, passkey or encryption key.

Access requests are routed to the Operations Manager. Typically, access is controlled through the addition of individual user accounts to established groups within Okta or Google Workspace.

Employee status data is used to facilitate the provisioning and removal of user accounts in the system. Upon termination, employees' access to systems is removed within 24 hours.

Annual access reviews of individual accounts and permissions on key systems are performed by authorized individuals, as appropriate, to evaluate whether access is still required. Remediation is taken, as necessary, based on the review.

Policies and standards have been established and implemented to enforce appropriate user account password expiration, length, complexity and history. PostHog personnel are required to follow the PostHog Password Policy for all domains as well as local user accounts for all assets.

Data Transmission

Customers access the PostHog instance through a web browser. TLS 1.2 or higher is required. Users authenticate access through a username and password or through their corporate single sign-on (SSO) identity provider.

Remote Access

A virtual private network (VPN) requiring MFA is used for all remote access to PostHog's internal network, ensuring that data is encrypted in transit when sent across the internet from a Company computer system.

Access to the PostHog infrastructure requires the use of MFA and is limited to a select few PostHog Development Operations team members and the CTO. All PostHog infrastructure access is logged, and customer data can only be accessed through the app layers of the infrastructure.

Physical Media and Data Destruction

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, printouts and other similar items used to process, store and/or transmit sensitive data are properly disposed of in accordance with measures established by PostHog.

Physical media (printouts and other physical media) are disposed of by one of the following methods:

- Shredded, using crosscut shredders
- Placed in locked shredding bins for a private contractor to come onsite and crosscut shred, witnessed by PostHog personnel throughout the entire process
- Incineration witnessed by PostHog personnel onsite at a private contractor's incineration site.

Electronic media (hard drives, tape cartridges, CDs, printer ribbons, flash drives, printer and copier hard drives, etc.) are disposed of by one of the following methods:

- Degaussing – a method to magnetically erase data from magnetic media
- Destruction – a method of destroying magnetic media; media is physically dismantled by methods of crushing, disassembling, etc., ensuring that the media has been physically destroyed so that no data can be pulled.

Third-Party Access and Due Diligence

PostHog uses third-party services that store and provide computing services to run its application. None of these system service providers have access to PostHog data on a day-to-day operational basis. All third-party service providers' in-scope systems and processes have SOC 2 Type 2 reports or have provided evidence of security controls and practices otherwise deemed acceptable by PostHog management. PostHog reviews the security reports for each of these organizations on an annual basis.

PostHog relies on third parties to perform a range of services and provide products. As such, PostHog performs due diligence to ensure that third parties have appropriate internal controls in place to protect PostHog's customer data. To ensure that appropriate controls are in place at third parties, PostHog executive management reviews the following as necessary:

- SOC 1 and/or SOC 2 reports
- Background checks, including client references and independent sources
- Staffing experience and expertise
- Internal controls
- Financial condition and annual reports
- Insurance coverage
- Privacy policies.

AVAILABILITY

Processing Capacity Management

Performance management and capacity monitoring tools are used to provide real-time information to the engineering team. Alert levels are established based on asset priority and failover capability for load-balanced and redundant components. Alerts may be in the form of a yellow or red color indicator on the operator console. The automatic creation of a problem ticket in the service management system for investigation and resolution, or an automated text and email to the on-call IT operations lead, is acceptable.

CONFIDENTIALITY

The Data Classification and Data Retention policies and relevant security and confidentiality policies describe how information is designated as confidential and ceases to be confidential. The handling, destruction, maintenance, storage, backup, distribution and transmission of confidential information is documented in the Data Classification and Data Retention policies, PostHog's general business terms and, in some cases, in customer and business partner-specific contracts and service-level agreements.

Confidentiality policies and processes have been implemented to limit access to logical input routines and physical input media to authorized individuals. Each type of confidential information is classified, handled, secured, retained and disposed of. All non-public customer information is confidential. Data that carries a confidential classification is subject to the Company's information security policy, which defines protection requirements, access rights and access restrictions, as well as retention and destruction requirements. Customer, vendor and business partner information is presumed to be confidential (as a default).

As part of its standard process for establishing service levels and operational protocols with vendors or business partners, PostHog evaluates data shared between the two organizations and agrees on what is confidential. PostHog also requests that business partners disclose their security, data classification and retention policies to ensure that PostHog's data is afforded the proper retention and information protection. The CTO and Vice President of Operations and Marketing are responsible for maintaining and updating confidentiality, system security and related policies.

At the time of hire or affiliation, the Code of Conduct and Confidential Information and Invention Assignment Agreement (or similar intellectual property or confidentiality agreement) that employees and contractors are required to sign prohibit any disclosures, beyond the extent authorized, of information or other data to which the employee is granted access. PostHog's business partners are also subject to nondisclosure agreements or other contractual confidentiality provisions, as outlined in the Business Associate Agreement. Customer contracts, service-level agreements and vendor contracts are negotiated before performance or receipt of service and formally signed off by management, legal, and operations as applicable.

Customers, groups of individuals or other entities are restricted from accessing confidential information other than their own. Users, contractors or vendors who have the ability to access confidential information are properly authorized or supervised, in line with the Company's employees. The information supervisor for a business unit determines whether users require access to confidential information to perform specific job functions.

Data Retention

Retention periods, and policies for ensuring retention during the specified period and proper disposal of data at the end of that period, are also outlined in the Data Classification and Data Retention policies. The retention period assigned to data is based on the (1) classification of the data, (2) regulatory requirements and legal statutes and (3) the general requirements of the business. During the designated retention period, PostHog ensures that backup media

(whether offline or online) is stored in a protected environment for the duration of the designated document retention period. Computer backup media is included. When the retention period has ended, PostHog destroys the information securely. Electronic information and other information are disposed of securely by proven means.

Risk Assessment Process

PostHog maintains a detailed inventory of all information systems. All assets are assigned ownership by a designated department or team within the entity and prioritized based on the asset's business value and criticality to the organization. Information and data assets are subject to the Data Classification and Data Retention policies that define parameters for the ownership, classification, security, storage and retention of data. Software and hardware assets are subject to the information systems management policy that defines parameters for the acquisition, development, maintenance, security and disposal of information system assets.

On an annual basis, the Information Security team performs a risk assessment that identifies internal and external threats and vulnerabilities to the organization. Information system assets are analyzed to identify associated threats to those assets and vulnerabilities that may be exploited. The resulting risks are then scored based on their likelihood and potential impact to the organization. The assessment includes consideration of the inherent and residual risks that may reside with external parties and the controls to address those risks. Specific policies and procedures are in place to assess and manage the requisition and engagement of vendors or business partners, with consideration for the threats and vulnerabilities such relationships may present.

Results of the risk assessment are evaluated by the CTO annually, against criteria for risk acceptance to identify new or existing protective measures and develop or enhance information security policies and procedures.

Information and Communication Systems

PostHog has an information security policy to help ensure employees understand their individual roles and responsibilities concerning processing and controls and ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of Slack and email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of a problem. PostHog uses checklists to help facilitate the upload of user information to the appropriate repository, in accordance with the user's instructions.

Monitoring

System Monitoring

As defined within the Application Logging and Monitoring Policy, the Infrastructure and Engineering teams perform monitoring to identify significant system events and conditions. Automated tools are in place to aggregate and analyze system and security event logs. System capacity, reliability, availability, application performance, response time, error rate and running services are all monitored, and metrics are collected and analyzed.

PostHog monitors its endpoints through third-party tools and follows up with individuals as needed until the correct configuration has been successfully installed.

Incident Response

The Incident Response Plan (IRP) comprises tactical procedures to help triage, contain, monitor or eradicate a security incident, including procedures to do the following:

- Respond to, recover from and restore normal business operations in a timely manner, with minimal or no business interruption or loss of data
- Continuously improve the cybersecurity risk management program to limit the likelihood and impact of future incidents based on lessons learned from the Company's own experiences and those of others
- Communicate with employees, stakeholders, regulators and other constituents in a structured manner about the nature of the security incident, impact to the organization and others (if applicable), and the corrective action taken to recover.

Virus Detection and Prevention

Antivirus software is required to be installed on all PostHog servers and workstations. Settings are preconfigured for automatic updates and locked to prevent any user tampering or disabling. Email filtering software is in place to restrict and reject emails that contain certain malicious file types, including executable files.

Vulnerability Assessment and Penetration Test

PostHog employs a third-party organization to conduct weekly internal vulnerability assessments, as well as annual penetration tests against production systems to determine if the system can be penetrated through known vulnerabilities. Management and the security team, as applicable reviews the results of the vulnerability assessments and penetrations tests and develops action plans to remediate critical and high-risk findings.

USE OF SUBSERVICE ORGANIZATION AND COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

PostHog uses AWS to perform cloud hosting services.

PostHog monitors the effectiveness of controls at the subservice organization by performing the following monitoring controls:

- Reviewing the most recently available SOC reports (type 2) on the subservice organization's system.
- Obtaining bridge letters from the subservice organization to obtain assurance that controls at the subservice organization are operating as intended and no significant changes were made since the subservice organization's most recent report was issued.
- Monitoring external communications (such as customer complaints) relevant to the services provided by the subservice organization.

Complementary user entity controls (CUECs) are identified in the subservice organization's SOC reports. PostHog reviews all applicable CUECs and ensures that controls have been implemented to satisfy the applicable CUECs, as necessary.

The following are applicable trust services criteria that are intended to be met by controls at the subservice organization and the types of controls expected to be implemented at the subservice organization that are necessary to meet the applicable trust services criteria, alone or in combination with controls at PostHog.

Security Category	
Criteria	*Controls expected to be in place by AWS*
CC6.4 – The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	AWS is responsible for restricting physical access to datacenter facilities, backup media, and other system components, including firewalls, routers and servers where PostHog's Analytics Platform resides.
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	AWS has appropriate controls in place to protect PostHog from threats from sources outside its system boundaries.
CC7.1 – To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities and (2) susceptibilities to newly discovered vulnerabilities.	AWS has appropriate controls in place for detecting security incidents and notifying PostHog when a security incident occurs.
CC7.2 – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	AWS has appropriate controls in place for monitoring PostHog production system for anomalies that are indicative of malicious acts.
CC7.3 – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	AWS has appropriate controls in place for evaluating security incidents and notifying PostHog if an incident is detected.

Availability Category	
Criteria	*Controls expected to be in place by AWS*
A1.2 – The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains and monitors environmental protections, software, data backup processes and recovery infrastructure to meet its objectives.	AWS has appropriate environmental controls in place to protect datacenters housing PostHog's data and to perform and monitor backup processes.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

The applicable trust services criteria and related control activities are included in Section IV of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section IV. Although the applicable trust services criteria and related controls are included in Section IV, they are, nevertheless, an integral part of PostHog's description of its Analytics Platform.

Trust Services Criteria for Which PostHog Relies on the Subservice Organization

PostHog's system, as described above, addresses all of the applicable Trust Services Criteria related to the security, availability, and confidentiality categories, with the exception of the following criterion for which PostHog relies on the subservice organization to meet its service commitments and system requirements related to its Analytics Platform.

- CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. AWS is responsible for the physical security of infrastructure housing PostHog customer data.

Trust Services Criteria Not Applicable to the System

The Company's operations address all applicable trust services criteria related to the security, availability and confidentiality categories.

Significant System Changes

There were no significant system changes to the PostHog Analytics Platform throughout the period June 1, 2025 to May 31, 2026.

Complementary User-Entity Controls

PostHog's services were designed with the assumption that certain controls would be implemented by user entities. These controls should be in operation at user entities to complement PostHog's controls. The user entity controls subsequently presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. User entities of PostHog's system should maintain controls for:

1. Designating individuals for authorizing access to the PostHog Analytics Platform
2. Periodically reviewing their customer access lists to the PostHog Analytics Platform and informing PostHog of any access change requests
3. Applying logical access security controls, data encryption controls and related procedures to their network connected equipment
4. Protecting their equipment against infection by computer viruses, malicious codes and unauthorized software

User-Entity Responsibilities

The controls below highlight the user entity responsibilities that the users of PostHog's services must perform to benefit from utilizing PostHog's system but do not affect PostHog's ability to meet its service commitments and system requirements.

1. Notifying PostHog management immediately of any employee termination that would require a revocation of logical access to the PostHog Analytics Platform
2. Implementing systems to protect against security and availability threats from sources outside the boundaries of the system
3. Complying with their contractual obligations

4. Ensuring the supervision, management and control of the use of PostHog's services by their personnel
5. Ensuring that procedures are in place for developing, maintaining and testing their own business continuity plans

SECTION IV: INFORMATION PROVIDED BY THE INDEPENDENT SERVICE AUDITOR

PURPOSE AND OBJECTIVES OF THE REPORT

This report is intended to provide users of PostHog's Analytics Platform with information about controls at PostHog that may affect the security, availability, and confidentiality of user entities' data and to provide users with information about the suitability of the design and operating effectiveness of controls.

Our examination was restricted to the description of the system, the security, availability, and confidentiality categories and criteria and related control procedures specified in Section III and Section IV by PostHog management and was not extended to procedures described elsewhere in this report but not listed, or to procedures that may be in effect at the subservice organization or user entities. It is each user auditor's responsibility to evaluate this information in relation to the controls in place at each user entity. If certain complementary controls are not in place at the user entity and subservice organization, PostHog's controls may not compensate for such weaknesses.

The description of the system and selection of the categories are the responsibility of PostHog's management. Our responsibility is to express an opinion about whether:

1) the description presents PostHog's Analytics Platform that was designed and implemented throughout the period June 1, 2025 to May 31, 2026 in accordance with the description criteria.
2) the controls stated in the description were suitably designed throughout the period June 1, 2025 to May 31, 2026 to provide reasonable assurance that PostHog's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the user entities and subservice organization applied the complementary controls assumed in the design of PostHog's controls throughout that period.
3) the controls stated in the description operated effectively throughout the period June 1, 2025 to May 31, 2026 to provide reasonable assurance that PostHog's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization and complementary user entity controls assumed in the design of PostHog's controls operated effectively throughout that period.

TESTS OF OPERATING EFFECTIVENESS

Our tests of the operational effectiveness of controls were designed to cover a representative number of samples throughout the period June 1, 2025 to May 31, 2026, for each of the controls, which are designed to achieve the specific criteria. In selecting particular tests of the operational effectiveness of controls, we considered (a) the nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the categories and criteria to be achieved, (d) the assessed level of control risk and (e) the expected efficiency and effectiveness of the test.

Test	Description
Corroborative inquiry	Made inquiries of appropriate personnel responsible for the performance of the control activity and corroborated responses with management.
Observation	Observed the application of a specific control activity.
Inspection	Inspected system screenshots, configurations, documents, and reports indicating the performance of the control activity, often through the use of sampling.

In accordance with paragraph .36 of AT-C section 205, *Assertion-Based Examination Engagements* (AICPA, *Professional Standards*), we assessed the reliability of information produced or provided by the service organization for use in our engagement. This evaluation included obtaining evidence supporting the accuracy and completeness of such information and determining whether it was sufficiently precise and detailed for the intended purpose.

For tests of controls involving Information Produced by the Entity (IPE), including electronic data, we performed procedures to evaluate the reliability of the information utilized. This included IPE used by management and distributed to user entities, IPE relied upon by management in the execution of controls, and IPE used in support of our testing procedures. Based on the nature of the IPE, our procedures included:

- Inspecting relevant source documentation
- Reviewing the queries, scripts, or parameters used to generate the IPE
- Reconciling the IPE to its source data
- Inspecting the IPE for irregularities in sequencing or timing that might affect completeness or integrity

For tests of controls involving management's use of IPE, we further reviewed evidence of management's procedures, where applicable, to assess the validity of the IPE source and confirm the completeness, accuracy, and integrity of the associated data and reports.

For any exceptions noted under Test Result, refer to Management Responses to Auditor's Exceptions in Section V.

CONTROLS SPECIFIED BY POSTHOG, INC. AND TESTS OF OPERATING EFFECTIVENESS

Security: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

Availability: Information and systems are available for operation and use to meet the entity's objectives.

Confidentiality: Information designated as confidential is protected to meet the entity's objectives.

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
A1.1.1	Processing capacity and usage are monitored on a real-time basis in order to appropriately manage capacity demand and to enable the implementation of additional capacity to meet availability commitments.	Inspected processing capacity and usage systems to determine that processing capacity demand was monitored on a real-time basis to allow for the implementation of additional capacity to meet availability commitments.	No exceptions noted.	CC9.1; A1.1; A1.2
A1.1.2	A load balancer is used to automatically distribute incoming application traffic across multiple instances and availability zones.	Inspected the load balancer configuration to determine that a load balancer was used to automatically distribute incoming application traffic across multiple instances and availability zones.	No exceptions noted.	CC9.1; A1.1; A1.2
A1.1.3	New server instances are automatically provisioned when predefined capacity thresholds are met.	Inspected auto scale configurations to determine that new server instances were automatically provisioned when predefined capacity thresholds are met.	No exceptions noted.	CC9.1; A1.1; A1.2

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
A1.2.1	An automated email is sent to appropriate personnel when the backup process fails.	Inspected the email configuration from AWS for backup failures to determine that an automated email was sent to appropriate personnel when the backup process failed.	No exceptions noted.	CC9.1; A1.2
A1.3.1	The integrity and completeness of back-up information is tested on an annual basis.	Inspected backup restoration testing results to determine that the integrity and completeness of back-up information was tested on an annual basis.	No exceptions noted.	CC9.1; A1.3
C1.1.1	PostHog establishes written policies related to retention periods for the confidential information it maintains.	Inspected the Data Retention Policy to determine that the entity established written policies related to retention periods for the confidential information it maintains.	No exceptions noted.	CC5.3; CC6.5; C1.1; C1.2
C1.1.2	PostHog has established a Data Classification Policy to identify the types of confidential information possessed by the entity and types of protection that are required.	Inspected the Data Classification Policy to determine that the entity had established a policy to identify the types of confidential information possessed by the entity and types of protection that were required.	No exceptions noted.	CC5.3; C1.1
C1.1.3	New hires and contractors are required to sign a Confidential Information and Invention Assignment Agreement (or similar intellectual property and confidentiality agreements) upon being hired.	For a sample of new hires, inspected signed Confidential Information and Invention Assignment Agreements (or similar intellectual property and confidentiality agreements) to determine that the agreements were signed upon being hired.	No exceptions noted.	CC1.1; CC1.5; CC2.2; CC2.3; CC5.3; C1.1

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
		For a sample of new contractors, inspected signed Confidential Information and Invention Assignment Agreements (or similar intellectual property and confidentiality agreements) to determine that the agreements were signed upon being hired.	No exceptions noted.	
C1.1.4	Test data is used within the entity's platform test environments.	Inspected the entity's platform test environments to determine that test data was used.	No exceptions noted.	C1.1
C1.2.1	Customer data is deleted within 30 days of the customer requesting data be deleted.	For a sample of customer data deletion requests, inspected a query detailing the customer data deletion request date and the data deletion verified date to determine that customer data was deleted within 30 days of the request.	No exceptions noted.	CC6.5; C1.2
CC1.1.1	The entity has a documented Code of Conduct that includes its commitments to integrity and ethical values.	Inspected PostHog's Code of Conduct to determine that it included its commitments to integrity and ethical values.	No exceptions noted.	CC1.1; CC5.3
CC1.1.2	New hires are required to read and accept the Code of Conduct upon being hired.	For a sample of new hires, inspected signed acknowledgements to determine that the Code of Conduct was acknowledged by new hires upon hire.	No exceptions noted.	CC1.1; CC1.4; CC1.5; CC2.2; CC5.3

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC1.1.3	New hires are required to read and accept an Acceptable Use Policy upon being hired.	For a sample of new hires, inspected signed Acceptable Use Policies to determine that new hires were required to read and accept the agreements upon hire.	No exceptions noted.	CC1.1; CC1.5; CC2.2; CC5.2; CC5.3
CC1.1.4	New hires are required to pass a background check as a condition of their employment.	For a sample of new hires, inspected background checks to determine that background checks were completed for new hires as a condition of their employment.	No exceptions noted.	CC1.1; CC1.4
CC1.1.5	For contractors hired through a third party, the entity reviews background information provided from the third party, prior to onboarding contractors.	For a sample of contractors hired through a third party, inspected PostHog's review of the contractors' background information from the third party to determine that PostHog reviewed the information prior to onboarding contractors.	No exceptions noted.	CC1.1; CC1.4
CC1.2.1	The members of the board of directors (BOD) are independent of management.	Inspected the member biographies for the BOD to determine that the BOD included members that were independent of management.	No exceptions noted.	CC1.2; CC1.3

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC1.2.2	Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	Inspected the information security policy to determine that roles and responsibilities to oversee implementation of the information security policy across the organization had been defined.	No exceptions noted.	CC1.2; CC1.3; CC2.1; CC2.2; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC5.3
CC1.2.3	Management exercises oversight of security controls by reviewing security policies on an annual basis.	Inspected review evidence to determine that management exercised oversight of security controls by reviewing security policies and making recommendations on an annual basis.	No exceptions noted.	CC1.2; CC1.3; CC2.1; CC2.2; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC5.3
CC1.2.4	The CTO exercises oversight and independence of risk management activities by reviewing results of internal risk assessments on an annual basis.	Inspected review evidence to determine that the CTO exercised oversight and independence of risk management activities by reviewing results of internal risk assessments on an annual basis.	No exceptions noted.	CC1.2; CC1.3; CC2.1; CC2.2; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC1.2.5	The CTO reports to the BOD on annual basis.	Inspected the BOD's meeting minutes to determine that the CTO reported to the BOD on an annual basis.	No exceptions noted.	CC1.2; CC1.3; CC2.1; CC2.2; CC2.3; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2
CC1.3.1	The CTO reviews its organizational structure, reporting lines, authorities, and responsibilities on an annual basis.	Inspected the organizational chart and inquired with the CTO to determine that the CTO reviewed the organizational structure, reporting lines, authorities, and responsibilities on an annual basis.	No exceptions noted.	CC1.3; CC3.4
CC1.3.2	An organizational chart has been defined to appropriately document reporting lines.	Inspected the organizational chart to determine that reporting lines had been appropriately defined.	No exceptions noted.	CC1.3
CC1.4.1	Job requirements and responsibilities are documented in job descriptions.	Inspected an example open job description to determine that job requirements and responsibilities were documented.	No exceptions noted.	CC1.4; CC1.5; CC2.2

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC1.4.2	Security awareness training is provided to new hires and onboarded contractors within the first month of being onboarded and to all employees on an annual basis.	For a sample of new hires and onboarded contractors, inspected security awareness training confirmation forms to determine that security awareness training was completed within the first month of being onboarded. For one of the 13 sampled new hires and onboarded contractors, security awareness training was not completed within the first month of being onboarded.	Exceptions noted.	CC1.4; CC1.5; CC2.2; CC5.2
		For a sample of current employees, inspected security awareness training confirmation forms to determine that security awareness training was completed on an annual basis.	No exceptions noted.	
CC1.4.3	Managers are required to complete performance appraisals for direct reports at least annually.	For a sample of current employees, inspected annual performance appraisals to determine that performance appraisals were completed by managers.	No exceptions noted.	CC1.4; CC1.5; CC2.2
CC2.1.1	The entity has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Inspected the Information Security Policy to determine that policies and procedures to support the functioning of internal control were defined.	No exceptions noted.	CC2.1; CC2.2; CC3.1; CC5.1; CC5.2; CC5.3; CC6.1; CC9.1

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC2.1.2	An architecture diagram exists to document system boundaries to support the functioning of internal control.	Inspected the architecture diagram to determine that the system boundaries to support the functioning of internal control were documented.	No exceptions noted.	CC2.1; CC5.2; CC6.1
CC2.1.3	A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	Inspected the risk assessment to determine that a risk assessment was completed during the period and identified and ranked potential threats to the system.	No exceptions noted.	CC2.1; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC9.1
CC2.2.1	The entity has incident response policies and procedures in place that include plans for escalating to internal personnel.	Inspected PostHog's Incident Response Plan and procedures to determine that the policies and procedures included plans for escalating to internal personnel.	No exceptions noted.	CC2.2; CC4.2; CC5.1; CC5.3; CC7.1; CC7.2; CC7.3; CC7.4; CC7.5; CC9.1
CC2.2.2	Internal personnel have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel via the Incident Response Plan, which is posted on the company intranet.	Inspected the Incident Response Plan and company intranet to determine that the Plan was posted on PostHog's intranet and included information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.	CC2.2; CC5.3
CC2.3.1	The entity communicates its security commitments to external users via the Terms of Service and Privacy Policy, which are publicly available on the company website.	Inspected the Terms of Service and Privacy Policy, that are public to all customers via the Company website, to determine that PostHog communicated its responsibilities for security.	No exceptions noted.	CC2.3; CC9.2

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC2.3.2	Agreements are established with key vendors that include clearly defined terms, conditions, and responsibilities which include confidentiality requirements.	For a sample of key vendors, inspected executed agreements to determine that the agreements outlined requirements, including terms, conditions, and responsibilities which include confidentiality requirements.	No exceptions noted.	CC2.3; CC9.2
CC3.1.1	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk assessment policy to determine that PostHog had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.	CC2.1; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC5.3; CC9.1
CC3.1.2	When identifying risks to include in the risk assessment, the entity considers relevant laws and regulations specific to the types of data it possesses (i.e. Protected Health Information, Personally Identifiable Information, etc.).	Inspected the completed risk assessment to determine that PostHog considered relevant laws and regulations specific to the types of data it possesses, when identifying risks to include in the risk assessment.	No exceptions noted.	CC2.1; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC9.1
CC3.2.1	Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected management's remediation plan to determine that management prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.	CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC9.1

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC3.2.2	Management monitors key vendors on an annual basis by either obtaining and reviewing the vendors' most currently available SOC reports or by performing other monitoring procedures.	For a sample of key vendors, inspected management's annual evaluation of the vendor to determine that management either obtained and reviewed the vendors' most currently available SOC report or performed other monitoring procedures.	No exceptions noted.	CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC9.2
CC3.3.1	Web application vulnerability scans are performed on a weekly basis to identify vulnerabilities, and management takes action to resolve critical and high-risk vulnerabilities, in a timely manner.	For a sample of weeks, inspected web application vulnerability scan results to determine that vulnerability scans were performed.	No exceptions noted.	CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC6.8; CC7.1; CC7.2; CC7.3; CC7.4; CC9.1
		Attempted to inspect resolution documentation to determine that management took action, as necessary, to resolve critical or high-risk vulnerabilities in a timely manner. Through corroborative inquiry with PostHog management and inspection of a sample of web application vulnerability scans, it was determined that no high-risk or critical vulnerabilities were identified during the report period.	The circumstances that warrant the operation of this control did not occur during the period covered by the examination and, therefore, no testing was performed.	

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC3.3.2	Web application penetration tests are performed by an independent third party on an annual basis, and management takes action to resolve critical and high-risk vulnerabilities in a timely manner.	Inspected the web application penetration test results to determine that a web application penetration test was performed by an independent third party annually.	No exceptions noted.	CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC6.8; CC7.1; CC7.2; CC7.3; CC7.4; CC9.1
		Inspected resolution documentation for all critical and high vulnerabilities to determine that management took action, as necessary, to resolve critical and high-risk vulnerabilities in a timely manner.	No exceptions noted.	
CC4.1.1	Access reviews for cloud infrastructure, version control and the PostHog Analytics Platform are performed on an annual basis.	Inspected the cloud infrastructure, version control and PostHog Analytics Platform access review documentation to determine that access reviews were completed on an annual basis.	No exceptions noted.	CC4.1; CC4.2; CC5.1; CC5.2; CC6.2; CC6.3; CC6.5
CC4.1.2	Continuous monitoring is implemented for controls to assess the effectiveness of controls and detect associated risk items.	Inspected the continuous monitoring platform to determine that implemented controls were automatically monitored to assess the effectiveness of the controls and detect risk items.	No exceptions noted.	CC2.1; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC9.1
CC4.1.3	PostHog has a defined Application Logging and Monitoring Policy to ensure that appropriate controls are in place over the log collection, monitoring and alerting processes for applications.	Inspected the Application Logging and Monitoring Policy to determine that appropriate controls were defined for log collection, monitoring, and alerting.	No exceptions noted.	CC4.1; CC5.3; CC6.6; CC6.8; CC7.1; CC7.2; CC7.3; CC7.4; CC9.1

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC5.1.1	As part of its annual risk assessment, management linked the identified risks to controls that have been designed and operated to address them. New controls are considered for any risks not adequately addressed by existing controls.	Inspected the risk assessment that was completed during the period to determine that risks were linked to controls and that new controls were considered for any risks not adequately addressed by existing controls	No exceptions noted.	CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC9.1
CC5.3.1	Business and system recovery plans are documented, which provide roles and responsibilities and detailed procedures for recovery of systems to a known state per defined recovery time objectives (RTOs) and recovery point objectives (RPOs). Plans are tested annually.	Inspected business and system recovery plans to determine that business and system recovery plans were documented and included roles and responsibilities and detailed procedures for recovery of systems to a known state per defined RTOs and RPOs.	No exceptions noted.	CC5.3; CC7.4; CC7.5; CC9.1; A1.2; A1.3
		Inspected business and system recovery test results to determine that business and system recovery plans were tested annually.	No exceptions noted.	
CC6.1.1	SSH is required to access EC2 instances.	Inspected security group settings to determine that SSH was required to access EC2 instances.	No exceptions noted.	CC6.1; CC6.6; CC6.7; C1.1
CC6.1.2	Network segmentation is in place so that unrelated portions of the entity's information system are isolated from each other.	Inspected the network diagram to determine that network segmentation was in place and unrelated portions of PostHog's information system were isolated from each other.	No exceptions noted.	CC6.1; CC6.6

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC6.1.3	Multi-factor authentication (MFA) is required to access the AWS Management Console.	Inspected AWS Management Console configurations to determine that MFA was required to access AWS.	No exceptions noted.	CC6.1; CC6.6; CC6.7; CC6.8; C1.1
CC6.1.4	Administrator access to AWS is restricted to appropriate personnel.	Inspected the list of users with administrator access to the AWS environment to determine that access was restricted to appropriate personnel.	No exceptions noted.	CC6.1; CC6.6; CC6.7; CC6.8; C1.1
CC6.1.5	AWS root account password standards are established to enforce the following: -complexity requirements -minimum length	Inspected minimum password requirements for the AWS root account to determine that AWS enforced the following password standards: -complexity requirements -minimum length	No exceptions noted.	CC6.1
CC6.1.6	AWS login for internal user accounts is managed through Single Sign-On (SSO).	Inspected AWS authentication configurations to determine that internal user accounts were managed through SSO.	No exceptions noted.	CC6.1; CC6.6; CC6.7
CC6.1.7	External users are required to authenticate to the PostHog Analytics Platform using their username and password or via SSO.	Inspected the authentication screen for the PostHog Analytics Platform to determine that external users were required to authenticate to the Platform using their username and password or via SSO.	No exceptions noted.	CC6.1; CC6.6; CC6.7

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC6.1.8	Super user access to the PostHog Analytics Platform is restricted to appropriate internal personnel.	Inspected the list of users with super user access to the PostHog Analytics Platform to determine that access was restricted to appropriate internal personnel.	No exceptions noted.	CC6.1; CC6.6; CC6.7; CC6.8; C1.1
CC6.1.9	Internal users are required to authenticate to the PostHog Analytics Platform using SSO.	Inspected configurations for the PostHog Analytics Platform to determine that employee access required SSO.	No exceptions noted.	CC6.1; CC6.3; CC6.6; CC6.7
CC6.1.10	Accessing the AWS root account requires MFA.	Inspected access configurations to the AWS root account to determine that MFA was required.	No exceptions noted.	CC6.1; CC6.6; CC6.7; CC6.8; C1.1
CC6.1.11	Role-based security is in place for internal and external platform users.	Inspected the PostHog Analytics Platform configurations to determine that role-based security was in place for internal and external platform users.	No exceptions noted.	CC6.1; CC6.3
CC6.1.12	Administrator access to AWS RDS databases for storing customer data is restricted to appropriate personnel.	Inspected the list of users with administrator access to the AWS RDS databases storing customer data to determine that administrator access was restricted to appropriate personnel.	No exceptions noted.	CC6.1; CC6.6; CC6.7; CC6.8; C1.1
CC6.1.13	Customer data at rest is encrypted.	Inspected the AWS RDS environment and S3 bucket configurations to determine that customer data was encrypted at rest.	No exceptions noted.	CC6.1; CC6.7; C1.1

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC6.1.14	Full-disk encryption is implemented for all workstations and laptops.	For a sample of workstations and laptops, inspected encryption settings to determine that full-disk encryption was implemented.	No exceptions noted.	CC6.1; CC6.7; C1.1
CC6.1.15	AWS IAM roles are configured to restrict permissions to cloud resources to appropriate personnel.	Inspected AWS IAM role assignments to determine that permissions to cloud resources were restricted to appropriate personnel.	No exceptions noted.	CC6.1; CC6.6; CC6.7; CC6.8; C1.1
CC6.1.16	The PostHog Analytics Platform's password standards are established to enforce the following: -minimum length -account lockout.	Inspected the PostHog Analytics Platform's password standards to determine that the following password standards were enforced: -minimum length -account lockout.	No exceptions noted.	CC6.1
CC6.1.17	External users can implement MFA on their accounts in order to require two forms of authentication prior to authentication to the PostHog Analytics Platform.	Inspected the PostHog Analytics Platform's configurations to determine that external users could implement MFA for users prior to authenticating to the PostHog Analytics Platform.	No exceptions noted.	CC6.1; CC6.6; CC6.7
CC6.1.18	The PostHog Analytics Platform's user passwords are stored using a salted password hash.	Inspected password storage encryption configurations to determine that external users' passwords for the PostHog Analytics Platform were stored using a salted password hash.	No exceptions noted.	CC6.1; CC6.6; CC6.7; C1.1

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC6.2.1	Prior to granting new hires and contractors access to system resources, an access request form must be approved by the Operations Manager.	For a sample of new hires, inspected onboarding checklists to determine that access requests were approved by the Operations Manager.	No exceptions noted.	CC6.2; CC6.3
		For a sample of contractors, inspected onboarding checklists to determine that access requests were approved by the Operations Manager.	No exceptions noted.	
CC6.2.2	An off-boarding checklist is completed for terminated employees, documenting access had been removed within one business day of the termination date.	For a sample of terminated employees, inspected off-boarding checklists to determine that a checklist was completed, documenting access had been removed within one business day of the termination date.	No exceptions noted.	CC6.2; CC6.3; CC6.5
		For a sample of terminated employees, inspected network, application, and database listings, as applicable, to determine that system access for terminated employees had been removed.	No exceptions noted.	
CC6.5.1	When employees are terminated, workstations are wiped and re-purposed, prior to re-issuing the workstation to another employee.	For a sample of terminated employees, inspected off-boarding checklists to determine that workstations were wiped and re-purposed, prior to re-issuing the workstation to another employee.	No exceptions noted.	CC6.5; C1.2

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC6.6.1	Inbound and outbound traffic to AWS is appropriately restricted.	Inspected virtual private cloud (VPC) firewall rules to determine that inbound and outbound traffic to AWS was appropriately restricted.	No exceptions noted.	CC6.6; CC6.7
CC6.6.2	An intrusion prevention system (IPS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected and perform automated procedures to prevent an intrusion from compromising the network.	Inspected the IPS configurations within AWS GuardDuty and an example alert to determine that an IPS was in place to detect potential intrusions, alert personnel if an intrusion was detected and perform automated procedures to prevent an intrusion from compromising the network.	No exceptions noted.	CC6.6; CC6.8; CC7.1; CC7.2; CC7.3; CC7.4; CC9.1
CC6.6.3	Read/Write access to AWS S3 Buckets are configured to restrict public access.	Inspected AWS S3 Bucket access configurations to determine Read/Write access was configured to restrict public access.	No exceptions noted.	CC6.6
CC6.6.4	The PostHog Analytics Platform has a maximum session time before requiring users to re-authenticate with their username and password.	Inspected the session maximum time setting to determine that the PostHog Analytics Platform has a maximum session time before required users to re-authenticate with their username and password.	No exceptions noted.	CC6.6
CC6.7.1	The PostHog Analytics Platform uses HTTPS to encrypt communications over the internet.	Inspected the login page for the PostHog Analytics Platform to determine that HTTPS was used to encrypt communications over the internet.	No exceptions noted.	CC6.7

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC6.7.2	Customer data is segregated from the data of other customers.	Inspected screenshots of a query requested within PostHog's GitHub repository to determine that customer data was segregated.	No exceptions noted.	CC6.7; C1.1
CC6.8.1	Antivirus software is installed on workstations and laptops to protect the network against malware.	For a sample of workstations, inspected antivirus software settings to determine that software was installed on workstations to protect the network against malware.	No exceptions noted.	CC6.8
CC6.8.2	Workstations operating system (OS) security patches are applied automatically.	For a sample of workstations, inspected auto update settings to determine that workstations were configured to automatically apply OS security patches.	No exceptions noted.	CC6.8
CC6.8.3	All AWS Elastic Cloud Compute (EC2) instances are running vendor-supported operating systems.	Inspected an AWS EC2 Amazon Machine Image (AMI) export to determine that all EC2 instances were running vendor-supported operating systems.	No exceptions noted.	CC6.8

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC6.8.4	Wiz is in place within the cloud environment to detect unauthorized file additions within the cloud environment, server instances, and application containers. Wiz is configured to alert personnel in the event that unauthorized file additions were made.	Inspected Wiz to determine that Wiz was in place and configured to detect unauthorized file additions within the cloud environment, server instances, and application containers.	No exceptions noted.	CC6.6; CC6.8; CC7.1; CC7.2; CC7.3; CC7.4; CC9.1
		Inspected Wiz alerting configurations to determine that Wiz was appropriately configured to alert personnel in the event that unauthorized file additions were made.	No exceptions noted.	
CC7.1.1	For PostHog application code changes, code reviews and approvals are performed by someone other than the person who made the code change.	For a sample of PostHog application code changes, inspected change request tickets to determine that code reviews and approvals were required to be completed by someone other than the person who made the change.	No exceptions noted.	CC7.1; CC8.1
CC7.2.1	Platform and application logs are monitored through automated tools and alerts are sent to appropriate personnel.	Inspected platform and application monitoring configurations to determine that automated alerts were sent to appropriate personnel.	No exceptions noted.	CC6.6; CC6.8; CC7.1; CC7.2; CC7.3; CC7.4; CC9.1; A1.1; A1.2
CC7.2.2	Cloudflare is configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created and sent to appropriate personnel.	Inspected Cloudflare configuration to determine that Cloudflare was configured to monitor web traffic and suspicious activity and send automated alerts to appropriate personnel.	No exceptions noted.	CC6.6; CC6.8; CC7.1; CC7.2; CC7.3; CC7.4; CC9.1; A1.1; A1.2

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC7.3.1	For all confirmed security incidents, PostHog documents and tracks the incident to resolution.	For a sample of confirmed security incidents, inspected incident response tickets to determine that PostHog documented and tracked the incident to resolution.	No exceptions noted.	CC7.3; CC7.4; CC7.5
CC7.4.1	For all confirmed security incidents, a root cause analysis is performed to determine what corrective actions are necessary to prevent the issue from occurring in the future.	For a sample of confirmed security incidents, inspected incident response documentation to determine that a root cause analysis was performed, and corrective actions were documented.	No exceptions noted.	CC7.4; CC7.5
CC7.5.1	Incident Response Plan testing is performed on an annual basis.	Inspected the results of Incident Response Plan test to determine that the Plan was tested on annual basis.	No exceptions noted.	CC5.3; CC7.5; CC9.1; A1.3
CC8.1.1	A Change Management Policy is defined to ensure that appropriate controls are in place over the acquisition, development, and maintenance of technology and its infrastructure.	Inspected the Change Management Policy to determine that a policy was defined to ensure that appropriate controls were in place over the acquisition, development, and maintenance of technology and its infrastructure.	No exceptions noted.	CC5.3; CC6.8; CC7.1; CC8.1
CC8.1.2	Version control software is used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.	Inspected the version control software to determine that software was used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.	No exceptions noted.	CC8.1

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC8.1.3	Access to the cloud source code version control system is restricted to appropriate personnel.	Inspected the list of users with access to the cloud source code version control system to determine that access was restricted to appropriate personnel.	No exceptions noted.	CC6.6; CC6.7; CC6.8; CC8.1
CC8.1.4	Code changes to the PostHog Analytics Platform are tested prior to implementation.	For a sample of code changes, inspected change request tickets to determine that code changes were tested prior to implementation.	No exceptions noted.	CC8.1
CC8.1.5	Separate environments are used for testing and production for the PostHog Analytics Platform.	Inspected the PostHog Analytics Platform testing and production environments to determine that separate environments were used.	No exceptions noted.	CC8.1
CC8.1.6	Access to merge pull requests without a code review is restricted to appropriate administrator personnel.	Inspected the list of code repository administrators to determine that access to merge pull requests without a code review was restricted to appropriate administrator personnel.	No exceptions noted.	CC8.1
CC9.1.1	Daily system snapshots are performed within AWS.	Inspected AWS RDS settings to determine that daily system snapshots were performed within AWS.	No exceptions noted.	CC9.1; A1.1; A1.2

Control Number	Description of PostHog's Controls	Test of Effectiveness	Test Result	Applicable Trust Services Criteria
CC9.1.2	Production data is replicated to a different availability zone to provide for recovery of data in the event that the primary availability zone is unavailable.	Inspected data replication configurations to determine that data was replicated to a different zone.	No exceptions noted.	CC9.1; A1.1; A1.2
CC9.2.1	An inventory of vendors is maintained that ranks vendors based on criticality.	Inspected the list of vendors to determine that an inventory of vendors was maintained based on criticality.	No exceptions noted.	CC9.1; CC9.2

Trust Services Criteria for Security, Availability, and Confidentiality and Mapping to Controls Specified by PostHog, Inc.

Criteria	Criteria Description	Control Activity Mappings
CC1.0 Control Environment		
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	C1.1.3; CC1.1.1; CC1.1.2; CC1.1.3; CC1.1.4; CC1.1.5
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	CC1.2.1; CC1.2.2; CC1.2.3; CC1.2.4; CC1.2.5
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CC1.2.1; CC1.2.2; CC1.2.3; CC1.2.4; CC1.2.5; CC1.3.1; CC1.3.2
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC1.1.2; CC1.1.4; CC1.1.5; CC1.4.1; CC1.4.2; CC1.4.3
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	C1.1.3; CC1.1.2; CC1.1.3; CC1.4.1; CC1.4.2; CC1.4.3
CC2.0 Communication and Information		
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CC1.2.2; CC1.2.3; CC1.2.4; CC1.2.5; CC2.1.1; CC2.1.2; CC2.1.3; CC3.1.1; CC3.1.2; CC4.1.2
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	C1.1.3; CC1.1.2; CC1.1.3; CC1.2.2; CC1.2.3; CC1.2.4; CC1.2.5; CC1.4.1; CC1.4.2; CC1.4.3; CC2.1.1; CC2.2.1; CC2.2.2
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	C1.1.3; CC1.2.5; CC2.3.1; CC2.3.2

Criteria	Criteria Description	Control Activity Mappings
CC3.0 Risk Assessment		
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CC1.2.2; CC1.2.3; CC1.2.4; CC1.2.5; CC2.1.1; CC2.1.3; CC3.1.1; CC3.1.2; CC3.2.1; CC4.1.2; CC5.1.1
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	CC1.2.2; CC1.2.3; CC1.2.4; CC1.2.5; CC2.1.3; CC3.1.1; CC3.1.2; CC3.2.1; CC3.2.2; CC4.1.2; CC5.1.1
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CC1.2.2; CC1.2.3; CC1.2.4; CC1.2.5; CC2.1.3; CC3.1.1; CC3.1.2; CC3.2.1; CC3.2.2; CC3.3.1; CC3.3.2; CC4.1.2; CC5.1.1
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	CC1.2.2; CC1.2.3; CC1.2.4; CC1.2.5; CC1.3.1; CC2.1.3; CC3.1.1; CC3.1.2; CC3.2.1; CC3.2.2; CC3.3.1; CC3.3.2; CC4.1.2; CC5.1.1
CC4.0 Monitoring Activities		
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	CC1.2.2; CC1.2.3; CC1.2.4; CC1.2.5; CC2.1.3; CC3.1.1; CC3.1.2; CC3.2.1; CC3.2.2; CC3.3.1; CC3.3.2; CC4.1.1; CC4.1.2; CC4.1.3; CC5.1.1
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	CC1.2.2; CC1.2.3; CC1.2.4; CC1.2.5; CC2.1.3; CC2.2.1; CC3.1.1; CC3.1.2; CC3.2.1; CC3.2.2; CC3.3.1; CC3.3.2; CC4.1.1; CC4.1.2; CC5.1.1
CC5.0 Control Activities		
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	CC1.2.2; CC1.2.3; CC1.2.4; CC1.2.5; CC2.1.1; CC2.1.3; CC2.2.1; CC3.1.1; CC3.1.2; CC3.2.1; CC3.2.2; CC3.3.1; CC3.3.2; CC4.1.1; CC4.1.2; CC5.1.1

Criteria	Criteria Description	Control Activity Mappings
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	CC1.1.3; CC1.2.2; CC1.2.3; CC1.2.4; CC1.2.5; CC1.4.2; CC2.1.1; CC2.1.2; CC2.1.3; CC3.1.1; CC3.1.2; CC3.2.1; CC3.2.2; CC3.3.1; CC3.3.2; CC4.1.1; CC4.1.2; CC5.1.1
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	C1.1.1; C1.1.2; C1.1.3; CC1.1.1; CC1.1.2; CC1.1.3; CC1.2.2; CC1.2.3; CC2.1.1; CC2.2.1; CC2.2.2; CC3.1.1; CC4.1.3; CC5.3.1; CC7.5.1; CC8.1.1
CC6.0 Logical and Physical Access Controls		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CC2.1.1; CC2.1.2; CC6.1.1; CC6.1.2; CC6.1.3; CC6.1.4; CC6.1.5; CC6.1.6; CC6.1.7; CC6.1.8; CC6.1.9; CC6.1.10; CC6.1.11; CC6.1.12; CC6.1.13; CC6.1.14; CC6.1.15; CC6.1.16; CC6.1.17; CC6.1.18
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	CC4.1.1; CC6.2.1; CC6.2.2
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	CC4.1.1; CC6.1.9; CC6.1.11; CC6.2.1; CC6.2.2
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	AWS is responsible for the physical security of infrastructure housing PostHog customer data.

Criteria	Criteria Description	Control Activity Mappings
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	C1.1.1; C1.2.1; CC4.1.1; CC6.2.2; CC6.5.1
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CC4.1.3; CC6.1.1; CC6.1.2; CC6.1.3; CC6.1.4; CC6.1.6; CC6.1.7; CC6.1.8; CC6.1.9; CC6.1.10; CC6.1.12; CC6.1.15; CC6.1.17; CC6.1.18; CC6.6.1; CC6.6.2; CC6.6.3; CC6.6.4; CC6.8.4; CC7.2.1; CC7.2.2; CC8.1.3
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	CC6.1.1; CC6.1.3; CC6.1.4; CC6.1.6; CC6.1.7; CC6.1.8; CC6.1.9; CC6.1.10; CC6.1.12; CC6.1.13; CC6.1.14; CC6.1.15; CC6.1.17; CC6.1.18; CC6.6.1; CC6.7.1; CC6.7.2; CC8.1.3
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	CC3.3.1; CC3.3.2; CC4.1.3; CC6.1.3; CC6.1.4; CC6.1.8; CC6.1.10; CC6.1.12; CC6.1.15; CC6.6.2; CC6.8.1; CC6.8.2; CC6.8.3; CC6.8.4; CC7.2.1; CC7.2.2; CC8.1.1; CC8.1.3
CC7.0 System Operations		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	CC2.2.1; CC3.3.1; CC3.3.2; CC4.1.3; CC6.6.2; CC6.8.4; CC7.1.1; CC7.2.1; CC7.2.2; CC8.1.1
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	CC2.2.1; CC3.3.1; CC3.3.2; CC4.1.3; CC6.6.2; CC6.8.4; CC7.2.1; CC7.2.2
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	CC2.2.1; CC3.3.1; CC3.3.2; CC4.1.3; CC6.6.2; CC6.8.4; CC7.2.1; CC7.2.2; CC7.3.1

Criteria	Criteria Description	Control Activity Mappings
CC7.4	The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.	CC2.2.1; CC3.3.1; CC3.3.2; CC4.1.3; CC5.3.1; CC6.6.2; CC6.8.4; CC7.2.1; CC7.2.2; CC7.3.1; CC7.4.1
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	CC2.2.1; CC5.3.1; CC7.3.1; CC7.4.1; CC7.5.1
CC8.0 Change Management		
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CC7.1.1; CC8.1.1; CC8.1.2; CC8.1.3; CC8.1.4; CC8.1.5; CC8.1.6
CC9.0 Risk Mitigation		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	A1.1.1; A1.1.2; A1.1.3; A1.2.1; A1.3.1; CC2.1.1; CC2.1.3; CC2.2.1; CC3.1.1; CC3.1.2; CC3.2.1; CC3.3.1; CC3.3.2; CC4.1.2; CC4.1.3; CC5.1.1; CC5.3.1; CC6.6.2; CC6.8.4; CC7.2.1; CC7.2.2; CC7.5.1; CC9.1.1; CC9.1.2; CC9.2.1
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	CC2.3.1; CC2.3.2; CC3.2.2; CC9.2.1
A1.0 Additional Criteria for Availability		
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	A1.1.1; A1.1.2; A1.1.3; CC7.2.1; CC7.2.2; CC9.1.1; CC9.1.2
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	A1.1.1; A1.1.2; A1.1.3; A1.2.1; CC5.3.1; CC7.2.1; CC7.2.2; CC9.1.1; CC9.1.2
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A1.3.1; CC5.3.1; CC7.5.1

Criteria	Criteria Description	Control Activity Mappings
C1.0 Additional Criteria for Confidentiality		
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	C1.1.1; C1.1.2; C1.1.3; C1.1.4; CC6.1.1; CC6.1.3; CC6.1.4; CC6.1.8; CC6.1.10; CC6.1.12; CC6.1.13; CC6.1.14; CC6.1.15; CC6.1.18; CC6.7.2
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	C1.1.1; C1.2.1; CC6.5.1

Section V: Other Information Provided by PostHog, Inc.

Management Responses to Auditor's Exceptions

Control Number	Control Activity	Exception Description	Management's Response to Auditor's Exceptions
CC1.4.2	Security awareness training is provided to new hires and onboarded contractors within the first month of being onboarded and to all employees on an annual basis.	For one of the 13 sampled new hires and onboarded contractors, security awareness training was not completed within the first month of being onboarded.	One onboarded contractor did not complete security awareness training within the required one-month window. The delay was isolated to this individual and did not reflect a breakdown in the underlying process; the contractor completed the training shortly after the one-month mark, and no security or related incidents resulted from the delay. To strengthen adherence to the one-month requirement, management has configured automated workflows that notify new hires and contractors of outstanding training via both Slack and email at 5, 8, 10, and 14 days from their start date. If training remains incomplete at 14 days, automated alerts are sent to management and the operations team via Slack, ensuring timely escalation and follow-up. These layered, automated reminders and escalation triggers are designed to prevent recurrence of this finding going forward.