pubnub

PubNub Inc.

System and Organization Controls (SOC) 3 Report

Report on PubNub’s Platform
Relevant to Security, Availability, Confidentiality, and Privacy

From the Period of July 1, 2024 through June 30, 2025

Frank, Rimerman + Co. LLP
certified public accountants

Table of Contents

Section I – Independent Service Auditor’s Report

PubNub Inc.
San Francisco, California

Scope

We have examined PubNub Inc.’s (the Company) accompanying assertion titled “Assertion of PubNub Inc. Management” (the Assertion) that the controls within PubNub’s Platform for real-time interactive apps (the Platform) were effective throughout the period July 1, 2024 to June 30, 2025 to provide reasonable assurance that PubNub Inc.’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*.

Attachment A within this report, titled “PubNub’s Platform Description Provided by PubNub Inc.” indicates complementary user-entity controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company’s service commitments and system requirements based on the applicable trust services criteria. Our examination did not include such complementary user-entity controls, and we have not evaluated the suitability of the design or the operating effectiveness of such controls.

Service Organization's Responsibilities

The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the Platform to provide reasonable assurance that the Company’s service commitments and system requirements were achieved. The Company has provided the accompanying assertion about the effectiveness of controls within the Platform. When preparing its assertion, the Company is responsible for selecting and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management’s assertion that controls within the Platform were effective throughout the period from July 1, 2024 to June 30, 2025 to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable services trust criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require us to plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination involves performing procedures to obtain evidence about the assertion and includes:

- Obtaining an understanding of the Platform and the Company's service commitments and system requirements.

- Assessing the risks the controls were not effective to achieve the Company's service commitments and system requirements based on the applicable trust services criteria.

- Performing procedures to obtain evidence about whether controls within the Platform were effective to achieve the Company's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

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

Our examination was not conducted for the purpose of evaluating the Company's cybersecurity risk management program. Accordingly, we do not express an opinion on any other form of assurance on its cybersecurity risk management program.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk the controls may become inadequate because of changes in conditions or the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the Company's Platform were effective throughout the period from July 1, 2024 to June 30, 2025, to provide reasonable assurance the Company's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Frank, Rimerman & Co. LLP

San Jose, California
August 21, 2025

Section II – Assertion of PubNub Inc. Management

We, as the management of PubNub Inc., are responsible for:

- Identifying PubNub's market-leading Platform for real-time interactive apps (the Platform) and describing the boundaries of the Platform. Our description of the boundaries of the Platform is presented in Attachment A, "PubNub's Platform Description Provided by PubNub Inc." and identifies the aspects of the Platform.

- Identifying our principal service commitments and system requirements. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B within this report, titled "The Principal Service Commitments and System Requirements".

- Identifying the risks that would threaten the achievement of our principal service commitments and system requirements that are the objectives of the Platform.

- Identifying, designing, implementing, operating, and monitoring effective controls over the Platform to mitigate risks that threaten the achievement of the principal service commitments and system requirements. In designing the controls over the Platform, we determined that certain trust services criteria can only be met if complementary user- entity controls are suitably designed and operating effectively throughout the period from July 1, 2024 to June 30, 2025.

- Selecting the trust services categories and associated criteria that are the basis of our assertion.

We confirm to the best of our knowledge and belief that the controls over the Platform were effective throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy set forth in the AICPA's TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*, and if user-entity controls assumed in the design of the Company's controls throughout the period from July 1, 2024 to June 30, 2025.

PubNub Inc.

/s/ Russell Lemelin
Chief Financial Officer
August 21, 2025

Attachment A – PubNub's Platform Description Provided by PubNub Inc.

Company

PubNub Inc. (the Company or PubNub) is a Software-as-a-Service (SaaS) company that provides a market leading platform for real-time interactive apps (PubNub Platform or the Platform) which powers real-time interactive experiences that drive engagement, retention, and monetization. The Platform product offerings are as follows:

Administration Portal – The PubNub Administration Portal (Admin Portal) allows customers to configure their use of the PubNub Application Program Interfaces (APIs), view billing and usage data, troubleshoot problems through a debug console, create custom functions, enable events and actions, and to access customer application analytics with PubNub Insights.

Real-Time Messaging – Real-Time Messaging (RTM) provides a high quality of service through orchestrated synchronization between multiple global Points-of-Presence (PoP) to deliver a consistent low-latency experience and continuous service operation even in the case of PoP failures or other catastrophic events. RTM utilizes various messaging patterns (such as publish/subscribe and streaming) to deliver data streams and device signaling. RTM establishes and maintains persistent connections to any device for low latency multi-directional communication between any internet-connected device.

The streams of messages can be used to power any kind of real-time application from a controlling device to sending streams of financial data, social updates, game player movement, or any other data that needs to be pushed between devices or servers. Data streams are composed of messages that can be sent across any number of channels to which any authorized device can subscribe. The RTM service provides a large collection of functionalities around the streams of data, including message storage, access control thought it's PubNub Access Manager or PAM, stream encryption (both end-to-end and point-to-point options), stream multiplexing, stream filtering, stream grouping (PubNub Stream Controller), and analytics on the data streams. The RTM service uses various gateways for message streams, including representational state transfer (REST) and mobile push notifications. RTM also provides a high quality of service through orchestrated synchronization between multiple global PoPs to deliver a consistent low-latency experience and continuous service operation even in the case of PoP failures or other catastrophic events.

PubNub Functions and Integrations – PubNub Functions allows customers to deploy code into the PubNub Platform to add application business logic directly into the network. Messages can be routed, filtered, aggregated, augmented, and transformed "in flight". The customer code is bundled and then deployed to the PubNub network to run simultaneously in global PoPs as a deployed microservice, which processes messages as they enter and traverse the PubNub network. PubNub Functions also includes a key and value data store that replicates across PoPs, enabling the customer to maintain the application state while being deployed in various global PoPs.

PubNub Events and Actions – PubNub's Events and Actions enables customers to filter real-time events generated by users and devices interacting on the PubNub Platform, queue those events, and deliver them in seconds to a growing catalog of actions, which include webhooks, Amazon Simple Queue Service (SQS), and Amazon Kinesis.

PubNub Insights – PubNub Insights provides a dashboard for customers to see where their users are (down to city level), and identify the most active users and channels. Using Analyze with an artificial intelligence (AI) feature in PubNub Insights, customers can analyze how their application is being used, identify issues, and plan for the future, without having to spend additional time and resources.

PubNub Illuminate – PubNub Illuminate is a real-time decisioning and analytics product that allows users to define the metrics and key performance indicators (KPIs) they desire to monitor, set-up the conditions to evaluate and use to trigger actions they want to take — all in real-time as it happens.

Components of the Platform Used to Provide Services

The boundaries of the Platform are the specific aspects of the Company's infrastructure, software, people, processes and procedures, and data necessary to provide its services. Any infrastructure, software, people, and data indirectly supporting the services provided to customers by PubNub are not included within the boundaries of the Platform. The components directly supporting the services provided to customers are described below.

Infrastructure

PubNub’s infrastructure is hosted in Amazon Web Services, Inc. (AWS) data centers from which the Platform is deployed. PubNub PoPs are designed and built with redundant network infrastructure. PubNub also uses International Business Machines Corporation (IBM Cloud) services to store off-site production data and configuration files that are encrypted in transit and at rest. PubNub uses Redis Inc. (Redis Labs) and NetApp Inc. (NetApp) to manage its databases.

AWS, IBM Cloud, Redis Labs, and NetApp are responsible for operating, managing, and controlling various components of the virtualization layer and storage as well as the physical security and environmental controls. Through daily operations, the Company monitors the quality of AWS, IBM Cloud, Redis Labs, and NetApp performance. Controls operated by AWS, IBM Cloud, Redis Labs, and NetApp are not included in the scope of this report.

Software

PubNub leverages industry standard tools to support the Platform. There are three key categories of software tools used by PubNub: 1) system configuration and provisioning software, 2) source code management software, and 3) logging and monitoring software.

System configuration and provisioning software provide PubNub Engineering personnel with the capability to deploy secure and consistent configurations across different systems. This software tool provides PubNub with the ability to rapidly provision standard configurations and hardened baseline configurations for the deployment of the Platform.

Source code management software provides PubNub Engineering personnel with a repository to centrally store and manage code used in production. This tool allows code and scripts to be standardized and version controlled through the software development lifecycle (SDLC). The SDLC includes developing, testing, and approving changes to maintain quality standards for code development.

PubNub utilizes industry standard logging software to record all production Secure Shell (SSH) access to logs stored on the Company's Amazon ElastiCache instances. Access to the SSH logs is restricted to personnel authorized by the Vice President (VP) of Engineering and Senior Director of Information Technology (IT) and Information Security.

Monitoring software provides PubNub Engineering personnel with views for tracking the security, performance, and effectiveness of the network, systems, and applications used to support the Platform. Alerts are configured to notify Engineering personnel when components of the Platform operate outside acceptable thresholds. Engineering personnel monitor critical areas on a 24x7 basis.

People

The Company's organizational structure provides a framework for planning, executing, and controlling business operations. It starts with management and is supported by key department managers and team members to ensure the segregation of duties concept is applied across the Company with mitigating controls for support. The organizational structure assigns roles and responsibilities to provide for adequate staffing, security and efficiency of operations.

The Company follows a structured onboarding process to familiarize new personnel with the Company's processes, systems, security, practices, policies and procedures.

Data

All data used in the Platform is encrypted in-transit and encrypted at rest using industry-recommended protocols, algorithms, and key sizes.

Customer data is classified and handled in accordance with PubNub's security, availability, confidentiality, and privacy policies into three categories: restricted, confidential, and public, as documented in the Information Classification Table. The PubNub Platform collects and propagates message data. Customers are provided with software and documentation to enable them to encrypt their message data if they so choose. Data is retained based on requirements specified by the customer during the account setup and onboarding process. PubNub provides end-to-end encryption of all data using industry-standard cryptographic protocols designed to provide communications security.

The Company ingests user-submitted data, which may include PII, through a secure web interface using Transport Layer Security (TLS) and Hypertext Transfer Protocol Secure. The Company shares transactional data with trusted partners through secure authenticated channels such as Virtual Private Network (VPN), TLS, Secure File Transfer Protocol (SFTP), and secure shell (SSH) with applicable access control policy enforcement.

Policies and Procedures

The policies and procedures are a series of documents used to describe the controls implemented within the Company. The purpose of the policies and procedures is to describe the operating environment and define the practices performed on behalf of the customer. These procedures are divided into two high-level categories: manual procedures and automated procedures. Manual procedures are performed by personnel whereas automated procedures are performed by computer software. The Company has automated procedures for monitoring performance, uptime, availability, and security events and alerting Company personnel. The Company has also developed and documented procedures for investigating and responding to potential security incidents that are tracked in the internal ticketing system. The policies and procedures include risk management, information security, and information assets management, security and vulnerability management, and data classification and handling among others. The policies and procedures are available to all Company personnel.

Control Environment

The Company’s internal control environment is governed and managed by the Company’s Board of Directors (the Board), management, and other personnel working on the achievement of objectives related to the effectiveness and efficiency of the Company operations while being in compliance with applicable laws and regulations. PubNub management meets with the Board periodically to communicate the current state of the business, including security and compliance-related updates.

Management emphasizes the implementation and adherence to controls and ethical behavior throughout the Company. The overarching business principles and standards of conduct contained within the Employee Handbook define the core values of the integrity expected of personnel. These principles are supported by a set of Company-wide commitments, standards, and requirements defining how the Company is governed. The Company has also developed a set of security-related policies as well as operational procedures outlining Company requirements to protect and secure assets and data and to hold individuals accountable for their internal control responsibilities. The Company has established policies and practices related to employee recruiting, hiring, onboarding, training, and performance evaluation. The HR team ensures third-party background checks are performed and new hires are aware of their obligation to protect the Company’s information and customer data. Formal performance reviews are conducted annually to aid in the continuous improvement process for the employee and the control environment.

Communication and Information

Management is committed to maintaining effective communication with personnel, customers, and business partners. The Company has established security, availability, confidentiality, and privacy-related policies that note the roles, responsibilities, and overall rules to achieving the Company's information security goals. Company personnel participate in the security awareness training ensuring their awareness of Company policies and security requirements.

The Company informs customers of the Company's commitments to the security of the Platform and the confidentiality of the data stored within the Platform within Terms and

Conditions, Master Services Agreements (MSA), and availability commitments within Service Level Agreements (SLA), which are provided to customers as part of the standard contract. PubNub has also established a Privacy Policy, which discloses the Company's practices related to the collection, usage, and retention of customer personally identifiable information (PII). The Company's website contains the Platform description and tutorials describing the features and functionality of the Platform as well as the Terms and Conditions and Privacy Policy.

Risk Assessment

The Company understands the necessary balance between risk and control, and the intent of risk management is to reduce risk to an acceptable level. The Company attempts to reduce business risk through an annual information security risk assessment when management identifies critical assets, the threats facing those assets, and the likelihood and impact of the security of the assets that could be compromised. Management reviews applicable laws and regulations, and the impact of new laws and regulations on the Company, as well as risks related to significant changes in production systems, key personnel, or operational environment. Risks are reviewed, assigned an owner, and remediated within a timeframe based on criticality and Platform impact.

Monitoring

The Company has designated a team responsible for monitoring the effectiveness of internal controls in the normal course of business operations. Monitoring tools are used to identify anomalies and issues, as well as to detect intrusions and vulnerabilities. Deviations in the operations of internal controls, including security and availability events are reported to management. In addition, any customer issues are communicated to the appropriate personnel for triaging and resolution.

Management engages a third-party consultant to conduct an internal audit of the Company's internal controls. When changes to internal controls occur, they are evaluated, agreed upon by the control owners, documented, and communicated in the Company's intranet. Results from the internal control reviews are communicated to management.

Complementary User-Entity Controls (CUECs)

Security is a shared responsibility between the Company and its customers. The Platform was designed with the assumption certain controls would be implemented by the customers (user entities). Certain requirements can be met only if the CUECs are suitably designed and operating effectively, along with related controls at the Company. Platform users should consider whether the following controls have been placed in operation at their organizations:

User entities are responsible for:
User entities are responsible for the accuracy, quality, integrity, legality, reliability, and appropriateness of all data entered or uploaded to the Platform.

User entities are responsible for:
User entities affected by outages exceeding the SLA must notify the Company in writing within thirty (30) days after the end of the affected month in order to qualify for credit under the terms of the SLA.
User entities are responsible for complying with their contractual obligations to the Company.
User entities are responsible for ensuring their personnel adhere to the policies and procedures on the use of the Platform.
User entities are responsible for managing, rotating, and resetting passwords for all employee users with access to the Platform.
User entities are responsible for notifying the Company when user entity data should be securely removed from the Platform. Termination of a contract does not automatically result in the disposal of customer data.
User entities are responsible for managing access (including provisioning and removing access) to their account using the administrator account within the Platform.
User entities are responsible for ensuring that only authorized individuals have the ability to access, modify, and delete information from the Platform.
User entities are responsible for using the Admin Portal to monitor user access to the Platform.
User entities are responsible for determining whether or not to encrypt data sent to the Company’s servers.
User entities are responsible for securing and monitoring the user entity’s data and the usage of that data.
User entities are expected to notify the Company if they suspect or learn of unauthorized access to the Platform.
User entities are responsible for reporting unusual or exceptional usage of the Platform immediately.
User entities are responsible for reporting to the Company any incidents and breaches that may impact the Platform.
User entities are responsible for understanding the SLA for third-party systems they purchase from such vendors that are integrated with the Platform.

User entities are responsible for:
User entities are responsible for establishing and communicating their privacy and security policies to their users and getting consent from end users to provide any PII to the Company.
User entities are responsible for requesting the Company to restrict customer message data from being replicated outside of the United States or European Union.
User entities are responsible for amending or correcting inaccurate PII maintained by the Company through the Admin Portal.

Attachment B – The Principal Service Commitments and System Requirements

The Company makes service commitments to its customers and has established system requirements as part of the Platform. Some of these commitments are principal to the performance of the Platform and relate to the AICPA TSC relevant to the applicable trust services criteria. The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the Platform to provide reasonable assurance its service commitments and system requirements are achieved based on the applicable trust services criteria.

Service commitments to customers are documented and communicated in the MSA or Terms and Conditions, SLAs, and the Privacy Policy. The Terms and Conditions can be found at https://www.pubnub.com/trust/legal/terms-and-conditions/ and the Privacy Policy can be found at https://www.pubnub.com/trust/legal/privacy-policy/ on the Company's website. The commitments include but are not limited to security, availability, confidentiality, and privacy.

Availability

The Company has made commitments related to percentage uptime and connectivity for the Platform, as well as commitments related to service credits for instances of downtime.

The Company is architected in a manner to maintain the availability of its services through defined programs, processes, and procedures. Contingency plans and incident response procedures are maintained to reflect emerging continuity risks and lessons learned. Plans are tested, updated through the course of business, reviewed annually, and approved by Management.

Security, Confidentiality, and Privacy

The Company has made commitments related to securing and maintaining the confidentiality of customer data and complying with relevant laws and regulations, as well as commitments related to the collection, use, retention, and access to users' personal data. These commitments are addressed through measures including confidentiality terms, data encryption, authentication mechanisms, and other relevant security and privacy controls.

The Company has also implemented technical controls designed to prevent unauthorized access to or disclosure of content. Internally, confidentiality and privacy requirements are communicated to personnel through training and policies. Company personnel are required to attend data privacy and security awareness training, which includes information, policies, and procedures related to protecting customers' data. In addition, the Company monitors the third parties used through annual periodic reviews by evaluating performance against contractual obligations, including confidentiality and privacy commitments.

The Company has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in the Company system policies and procedures, system design documentation, and contracts with customers.

Information security policies define a Company-wide approach to how systems and data are protected. These policies include how the Platform is designed, developed, and operated, how the internal business systems and networks supporting the Platform are managed, and how personnel are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of various services provided by the Platform.