System and Organization Controls (SOC 3) Report

Independent Assurance Report on Controls at Service Organization

Krisp Technologies, Inc.

Contents

Գրանթ Թորնթոն Քնսալթինգ ՓԲԸ
Երևան Պլազա բիզնես կենտրոն
ՀՀ, ք. Երևան 0015
Գրիգոր Լուսավորչի 9
Հ. + 374 10 500 964
+ 374 10 500 961

Grant Thornton Consulting CJSC
Yerevan Plaza Business Center
9 Grigor Lusavorich Street,
Yerevan 0015, Republic of Armenia
T + 374 10 500 964
+ 374 10 500 961

Independent Assurance Report on the Description of Controls, their Design and Operating Effectiveness

To the Management of Krisp Technologies, Inc.

Scope

We have performed an independent reasonable assurance engagement on Krisp Technologies, Inc.'s description of its system entitled "Krisp Technologies, Inc.'s Application" on pages 8-15, for the period from 1 September 2022 to 31 August 2023 (the "System Description"), and on the design and operation of controls related to control objectives stated in the System Description, based on the criteria for the security, availability, processing integrity, confidentiality and privacy (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Krisp Technologies, Inc. uses subservice organizations 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 Krisp Technologies, Inc., to achieve Krisp Technologies, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Krisp Technologies, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organizations controls assumed in the design of Krisp Technologies, Inc.'s controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organizations' controls.

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

Management's Responsibilities

In "Krisp Technologies, Inc. Management Statement", Krisp Technologies, Inc. has provided a statement about the fairness of the presentation of the System Description and the design and operating effectiveness of the controls to achieve the related control objectives. Management of Krisp Technologies, Inc. is responsible for preparing the System Description and the accompanying Statement on pages 6-7, including the completeness, accuracy, and method of presentation of the System Description and the Statement, providing the services covered by the System Description, specifying the control objectives and stating them in the System Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Statement, and designing, implementing, documenting and effectively operating controls to achieve the stated System-related control objectives.

Our Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies International Standard on Quality Management 1 and accordingly maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on Krisp Technologies, Inc.'s System Description and on the design and operating effectiveness of the controls to achieve the related control objectives stated in the System Description, based on our procedures.

We conducted our engagement in accordance with the "*International Standard on Assurance Engagements 3000 (Revised): Assurance Engagements other than Audits or Reviews of Historical Financial Information"* issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, based on the criteria stated in management's Statement, the System Description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the System Description.

An assurance engagement to report on the service organization's system and the suitability of the design and operating effectiveness of controls involves performing procedures to obtain evidence about the fairness of the System Description presentation and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives, based on the criteria in management's Statement. The procedures selected depend on the service auditor's judgment, including the assessment of risks that the System Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the System Description. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the System Description were achieved. An assurance service of this type also includes evaluating the overall presentation of the System Description, suitability of the control objectives, and suitability of the criteria specified by the service organization in its assertion.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations of Controls

The System Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' environments and systems and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or failures, including the possibility of human error and circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability, processing integrity, confidentiality, and privacy will be achieved.

Examples of inherent limitations in an entity's security controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer;
- Ineffective controls at a vendor or business partner;
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Also, the projection to the future of any evaluation of the fairness of the presentation of the System Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are described on pages 6-7.

In our opinion, in all material respects:

- the System Description fairly presents Krisp Technologies, Inc.'s System as designed and implemented throughout the period from 1 September 2022 to 31 August 2023, in accordance with the description criteria;
- the controls related to the control objectives stated in the System Description were suitably designed throughout the period from 1 September 2022 to 31 August 2023 to provide reasonable assurance that Krisp Technologies, Inc.'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 Krisp Technologies, Inc.'s controls throughout the period from 1 September 2022 to 31 August 2023;
- the controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the System Description were achieved, operated effectively throughout the period from 1 September 2022 to 31 August 2023 to provide reasonable assurance that Krisp Technologies, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria and if the subservice organizations and user entities applied the complementary controls assumed in the design of Krisp Technologies, Inc.'s controls throughout the period from 1 September 2022 to 31 August 2023.

Grant Thornton Consulting CJSC

25 September 2023

Krisp Technologies, Inc.

Management Statement

Krisp Technologies, Inc. Management's Statement Regarding the Effectiveness of its Controls, Based on the Trust Services Principles and Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy

We have prepared the accompanying description of Krisp Technologies, Inc.'s System entitled "Krisp Technologies, Inc.'s Application", throughout the period from 1 September 2022 to 31 August 2023, for user entities of the services and their auditors who audit and report on such user entities' in the areas of security, availability, confidentiality, processing integrity and privacy and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks related to internal control related to security, availability, confidentiality, processing integrity and privacy.

Krisp Technologies, Inc. uses a subservice organization to provide data center facility and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Krisp Technologies, Inc., to achieve Krisp Technologies, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Krisp Technologies, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Krisp Technologies, Inc.'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 Krisp Technologies, Inc., to achieve Krisp Technologies, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Krisp Technologies, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Krisp Technologies, Inc.'s controls. The System description does not extend to the controls of the user entities as set out in "Terms of Use" at Terms of Use | Krisp.

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

- System description fairly presents Krisp Technologies, Inc.'s System during the period from 1 September 2022 to 31 August 2023 as it relates to controls of security, availability, confidentiality, processing integrity and privacy. The criteria we used in making this statement were that the System description:
  - presents how the System was designed and implemented to process relevant user entity data, including, if applicable:
    - types of services provided, including, as appropriate, the types of data processed;
    - the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities;
    - how the system captures and addresses significant events and conditions;
    - relevant control objectives and controls designed to achieve those objectives;
    - other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
  - includes relevant details of changes to Krisp Technologies, Inc.'s system during the period covered by the System Description;

  - does not omit or distort information relevant to Krisp Technologies, Inc.'s system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the Krisp Technologies, Inc.'s System that each individual user entity and its auditor may consider important in its own particular environment.

- controls related to the control objectives stated in the System Description were suitably designed and operating effectively throughout the period from 1 September 2022 to 31 August 2023 to achieve those control objectives, if the subservice organizations and user entities applied the complementary controls assumed in the design of Krisp Technologies, Inc.'s controls throughout the period from 1 September 2022 to 31 August 2023. The criteria we used in making this assertion are the following:
  - Risks that threaten the achievement of the control objectives stated in the System Description have been identified by the management of Krisp Technologies, Inc.;
  - Controls identified in the System Description would, if operated as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the System Description from being achieved;
  - Controls were consistently applied as designed, including manual controls were applied by individuals who have the appropriate competence and authority.
- System was protected against unauthorized access, use, or modification to achieve Krisp Technologies, Inc.'s commitments and system requirements;
- System was available for operation and use, to achieve Krisp Technologies, Inc.'s commitments and system requirements;
- System information is collected, used, disclosed, and retained to achieve Krisp Technologies, Inc.'s commitments and system requirements;
- System processing is complete, valid, accurate, timely, and authorized to meet Krisp Technologies, Inc.'s commitments and system requirements;
- Personal information is collected, used, retained, disclosed, and disposed to meet Krisp Technologies, Inc.'s commitments and system requirements, based on the Control Criteria.

Krisp Technologies, Inc. Management

20 September 2023

Krisp Technologies, Inc.’s System Description

Krisp Technologies, Inc. Background

Krisp Technologies, Inc. (hereinafter – the Company or Krisp), founded in 2018, is a software developer company of a machine-learning-based speech enhancement technology designed to turn background voice audio into crisp audio. The Company's technology automatically recovers lost sound packets during network transfers, mutes background noise, turns low bitrate audio to high-definition audio and makes the voice louder, helping contact centers, telecommunications, conferences, critical communications, and others to turn their existing audio devices into HD communication devices.

Control Environment

Krisp Technologies, Inc. management has identified the controls over the system throughout the period from 1 September 2022 to 31 August 2023 to achieve its commitments and system requirements related to the operation using the criteria for security, availability, and confidentiality (Control Criteria) set forth in the AICPA’s TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this, the management has selected a set of controls to provide reasonable assurance that:

- System is protected against unauthorized access, use, or modification to achieve Krisp Technologies, Inc.’s commitments and system requirements;
- System is available for operation and use, to achieve Krisp Technologies, Inc.’s commitments and system requirements;
- System information is collected, used, disclosed, and retained to achieve Krisp Technologies, Inc.’s commitments and system requirements;
- System processing is complete, valid, accurate, timely, and authorized to meet Krisp Technologies, Inc.’s commitments and system requirements;
- Personal information is collected, used, retained, disclosed, and disposed to meet Krisp Technologies, Inc.’s commitments and system requirements, based on the Control Criteria.

Scope

The scope of the systems covered in this report includes:

The key products of the Company are:

- Krisp Desktop for Windows/MacOS
- Krisp Pro (renamed from Krisp Teams)
- Krisp Enterprise.

The key organizational units (teams) of Krisp Technologies, Inc.:

- Research team
- PeopleOps team
- Product team
- Sales team (located in US)
- Marketing team
- Support (Customer Service) team
- Information Security team.

The key tools of the Company used for product development:

- Microsoft Azure
- OpenAI
- AWS
- JumpCloud
- Sendgrid
- Zendesk
- JIRA
- Google Data Studio
- Stripe
- Papertrail
- Sentry

Infrastructure

Krisp Technologies, Inc. infrastructure includes facilities, network, and hardware, as well as some system software (e.g., host operating system, virtualization software, etc.) that support the provisioning and use of these resources. Krisp Technologies, Inc. infrastructure is designed and managed in accordance with security compliance standards and Krisp Technologies, Inc. security policies.

Most of Krisp Technologies, Inc.'s servers are hosted at AWS. Only one server (dedicated for Research Team) is located in Yerevan office.

Locations

The locations covered in this report include:

- 2150 Shattuck Ave, Suite 1300, Berkeley, CA 94704, USA,
- 5/1 Hrachya Kochar Str, Yerevan, Armenia,
- 4/1 Marshal Baghramyan Ave, Yerevan, Armenia.

People

Krisp Technologies, Inc.'s organizational structure provides a framework for planning, executing and controlling business operations. Executive and senior leadership play important roles in establishing Krisp Technologies, Inc.'s tone and core values. The organizational structure assigns roles and responsibilities to provide for adequate staffing, security, efficiency of operations, and segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel.

The Company follows a structured on-boarding process to familiarize new employees with Krisp Technologies, Inc.'s tools, processes, systems, security practices, policies and procedures. Employees are provided with the set of the Krisp Technologies, Inc.'s policies and pass induction training to educate them as to their responsibilities concerning information security.

Customer Data

Krisp desktop app (Windows and Mac) processes all voice audio data on the end user's machine. This data never leaves the user's machine.

Krisp stores the following customer data in its cloud:

- Emails (if the customer is using email-based signup). No emails will be stored if customer is using device-based authentication,
- Team names,
- Payment history and invoices (credit card numbers are stored at Stripe),
- Analytics data,
- Aggregated statistics on time duration (in minutes) for which Krisp has been used,
- Microphone, speaker names which Krisp is being used with (e.g. AirPod),
- Krisp Desktop - Application name which Krisp has been used with (e.g. Zoom, Skype),
- Krisp Chrome Extension - The domain name which Krisp has been used with (e.g. meet.google.com).

Subservice Organizations

Krisp Technologies, Inc.'s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all the trust services criteria related to Krisp's services to be solely archived by Krisp control procedures. Accordingly, subservice organizations, in conjunction with the service, should establish their own internal controls or procedures to complement those of Krisp.

The following subservice organization controls should be implemented by AWS, Microsoft Azure, OpenAI and JumpCloud to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization Name	Relevant Control Criteria
AWS	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC6.8, CC7.1, CC7.2, CC7.4, CC7.5, CC9.1, A1.2, A1.3, C1.1
Microsoft Azure	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC6.8, CC7.1, CC7.2, CC7.4, CC7.5, CC9.1, A1.2, A1.3
OpenAI	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC6.8, CC7.1, CC7.2, CC7.4, CC7.5, CC9.1, A1.2, A1.3
JumpCloud	CC6.1, CC6.2, CC6.3, CC6.6, CC6.7, CC7.2, CC9.1, A1.2, A1.3

Accordingly, these identified complementary subservice organization controls are "carving-out" from the audit scope.

Availability

Krisp products have architected in a manner to maintain availability of its services through defined programs, processes, and procedures. The Business Continuity Program encompasses the processes and procedures by which Krisp Technologies, Inc. identifies, responds to, and recovers from a major event or incident within the environment. This program builds upon the traditional approach of addressing contingency management, incorporating elements of business continuity and disaster recovery plans while expanding to consider critical elements of proactive risk mitigation strategies. These strategies include continuous infrastructure capacity planning.

Contingency plans and incident response playbooks are maintained to reflect emerging continuity risks and lessons learned. Plans are tested and updated through the course of business, and the Krisp

Technologies, Inc. Business Continuity Program is regularly reviewed and approved by senior leadership.

Krisp Technologies, Inc. has identified critical system components required to maintain the availability of the system and recover services in the event of an outage. These components are replicated across multiple availability zones; authoritative backups are maintained and monitored to ensure successful replication.

Krisp application operates locally on the users' machines and most of the time does not need to connect to its backend. When it detects that it can no longer connect to the backend, it stops operating.

Krisp Technologies, Inc.'s backend infrastructure is entirely hosted on AWS, fully automated and monitored by continuous functional tests to detect any sort of downtime, protecting infrastructure needs and supporting availability commitments and requirements. Additionally, Krisp Technologies, Inc. maintains a capacity planning model to assess infrastructure usage and demands.

Security

Krisp Technologies, Inc. has established information security policies and there is an executive-level commitment to implement and follow the policies throughout the organization.

Information Security program is led by the Head of Security of Krisp Technologies, Inc.

Confidentiality

Krisp Technologies, Inc. is committed to protecting security and confidentiality of its customers' content, defined as "Security at Krisp" at Security at Krisp. Krisp Technologies, Inc. communicates its confidentiality commitment to customers in "Terms of use" at Terms of Use | Krisp.

Internally, confidentiality requirements are communicated to employees through training and policies. Employees are required to attend security awareness training, which includes information, policies, and procedures related to protecting customers' content. Krisp Technologies, Inc. monitors the performance of third parties through periodic reviews, which evaluate performance against contractual obligations, including confidentiality commitments.

Privacy

Krisp Technologies, Inc. is committed to protecting the personal data of its customers' content, defined as "Security at Krisp" at Security at Krisp and "Privacy Policy" at Privacy Policy | Krisp. Krisp Technologies, Inc. communicates its privacy commitment to customers in "Terms of use" at Terms of Use | Krisp.