Grant Thornton
An instinct for growth™

System and Organization Controls (SOC 3) Report

Report on the System relevant to Security, Availability, Confidentiality, Processing integrity and Privacy

Krisp Technologies, Inc.

For the period September 1st to September 25th, 2020

Contents

Report of Independent Accountants

To the Management of Krisp Technologies, Inc.

Scope and Approach

We have examined Krisp Technologies, Inc. management assertion that Krisp Technologies, Inc. maintained effective controls to provide reasonable assurance that:

- the Krisp Technologies, Inc. Application (hereafter the System) was protected against unauthorized access, use, or modification to achieve its commitments and system requirements;
- the Krisp Technologies, Inc. System was available for operation and use, to achieve Krisp Technologies, Inc.'s commitments and system requirements;
- the Krisp Technologies, Inc. System information is collected, used, disclosed, and retained to achieve Krisp Technologies, Inc.'s commitments and system requirements;
- the System processing is complete, valid, accurate, timely, and authorized to meet the Krisp Technologies, Inc.'s commitments and system requirements;
- personal information is collected, used, retained, disclosed, and disposed to meet the Krisp Technologies, Inc.'s commitments and system requirements.

During the period September 1st to September 25th, 2020, we have examined the System controls related to the operation using the criteria for the 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.

This assertion is the responsibility of Krisp Technologies, Inc. management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards by the American Institute of Certified Public Accountants. Those standards require that service auditor plan and perform the examination to obtain reasonable assurance about management's assertion, which includes:

- obtaining an understanding of Krisp Technologies, Inc.'s relevant security, availability, and confidentiality policies processes and controls;
- testing and evaluating the operating effectiveness of the controls; and
- performing other procedures as we considered necessary in the circumstances.

The nature, timing and extent of the procedures selected depended on our judgement, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

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

Inherent Limitations

This report 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, internal controls at a service organization may not prevent, or detect and correct, all errors or issues, 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 are achieved.

Examples of inherent limitations in an entity's security's 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 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 ineffective.

Opinion

In our opinion, Krisp Technologies, Inc. management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, processing integrity, confidentiality, and privacy.

Grant Thornton Consulting CJSC

September 25th, 2020

Management's Report of Its Assertion

Krisp Technologies, Inc. Management's Assertion Regarding the Effectiveness of Its Controls Over Its System and Based on the Trust Services Principles and Criteria for Security, Availability, and Confidentiality

We, as management of Krisp Technologies, Inc., are responsible for designing, implementing and maintaining effective controls over the Krisp application (System) to provide reasonable assurance that commitments and system requirements related to the System operation are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in security controls, an entity may achieve reasonable, but not absolute, assurance that security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations at Krisp Technologies, Inc.'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 Krisp Technologies, Inc.

Furthermore, projections of any evaluation of effectiveness to future periods are 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.

We have performed an evaluation of the effectiveness of the controls over the System throughout the period September 1st to September 25th, 2020 using criteria for the 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 evaluation, we assert that the controls were effective throughout the period September 1st to September 25th, 2020 to provide reasonable assurance that:

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

Our attached description of the Krisp Technologies, Inc.'s System boundaries identifies the aspects of the System covered by our assertion.

Krisp Technologies, Inc. Management

August 25th, 2020

Description of Krisp Technologies, Inc.

Krisp Technologies, Inc. Background

Krisp Technologies, Inc. (Company), 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 centres, telecommunications, conferences, critical communications, and others to turn their existing audio devices into HD communication devices.

Scope

The scope of the systems covered in this report includes:

The key products of Krisp Technologies, Inc.:

- Krisp Desktop for Windows/MacOS
- Krisp Teams
- Krisp Enterprise

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

- Research team
- Product team
- Sales team (located in US)
- Marketing team
- Support (Customer Service) team

During the course of gap analysis phase, the Company was in a process of recruitment of Chief Information Security Officer and IT Support Specialist.

The key tools of the Company used for product development:

- AWS
- Sendgrid
- Zendesk
- Google Data Studio
- Stripe
- Papertrail
- Sentry

Infrastructure

Krisp Technologies, Inc. infrastructure includes the facilities, network, and hardware as well as some operational software (e.g., host operating system, virtualization software, etc.) that support 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 onsite in Yerevan office.

Locations

The locations covered in this report include:

- 2150 Shattuck Ave., Suite 1300, Berkeley, CA 94704; and
- 5/1 Hrachya Kochar St., 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.

Krisp Technologies, Inc. follows a structured on-boarding process to familiarize new employees with corporatewide 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 the customer is using device-based authentication.
- Team names
- Payment history and invoices (credit card numbers are stored at Stripe)
- Analytics data
- Aggregated statistics minutes Krisp has been used for
- 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)

Availability

Krisp products are 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 app operates locally on the users' machines and most of the time doesn't 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, it's 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 the security and confidentiality of its customers' content, defined as "Customer data" at https://krisp.ai/security/#9 . Krisp Technologies, Inc. communicates its confidentiality commitment to customers in "Terms of use" at https://krisp.ai/terms-of-use/ .

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 "GDPR and Data Retention" at https://krisp.ai/security/#5 and "Privacy Policy" at https://krisp.ai/privacy-policy/ . Krisp Technologies, Inc. communicates its privacy commitment to customers in "Terms of use" at https://krisp.ai/terms-of-use/.