System and Organization Controls (SOC 3) Report
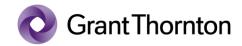
Independent Assurance Report on Controls at Service Organization

Podcastle, Inc.

Contents

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

To the Management of PODCASTLE, Inc.

Scope

We have performed an independent reasonable assurance engagement on Podcastle, Inc. (hereinafter – "Podcastle" or "the Company") description of its system entitled "Podcastle Platform" on pages 8-14, for the period from 1 March 2024 to 31 August 2024 (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*.

Podcastle 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 Podcastle, to achieve Podcastle's service commitments and system requirements based on the applicable trust services criteria. The description presents Podcastle's controls, the applicable trust services criteria, and the types of complementary subservice organizations controls assumed in the design of Podcastle'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 Podcastle, Inc., to achieve Podcastle's service commitments and system requirements based on the applicable trust services criteria. The description presents Podcastle's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Podcastle'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 *Podcastle, Inc. Management Statement*, Podcastle 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 Podcastle is responsible for preparing the 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.

![Grant Thornton]

Our Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Work Ethics and Code of Conduct 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 behavior.

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 *Podcastle'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,

Grant Thornton

Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Additionally, 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 Podcastle's System as designed and implemented throughout the period from 1 March 2024 to 31 August 2024, 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 March 2024 to 31 August 2024to provide reasonable assurance that Podcastle'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 Podcastle's controls throughout the period from 1 March 2024 to 31 August 2024,

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 March 2024 to 31 August 2024 to provide reasonable assurance that Podcastle'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 Podcastle's controls throughout the period from 1 March 2024 to 31 August 2024.

The detailed description of the controls is presented in *Appendix A - Tests of Controls, Findings and Recommendations*.

Grant Thornton Consulting CJSC

30 September 2024

PODCASTLE, Inc. Management Statement

PODCASTLE, 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 Podcastle, Inc. (hereinafter – "Podcastle" or "the Company") System entitled "Podcastle Platform", throughout the period from 1 March 2024 to 31 August 2024, 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.

Podcastle 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 Podcastle, to achieve Podcastle's service commitments and system requirements based on the applicable trust services criteria. The description presents Podcastle's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Podcastle'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 Podcastle, to achieve Podcastle's service commitments and system requirements based on the applicable trust services criteria. The description presents Podcastle's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Podcastle's controls. The System description does not extend to the controls of the user entities as set out in "Terms and conditions" Terms & Conditions | Podcastle.

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

System description fairly presents Podcastle's System during the period from 1 March 2024 to 31 August 2024 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 Podcastle's system during the period covered by the System Description,

does not omit or distort information relevant to Podcastle'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 Podcastle'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 March 2024 to 31 August 2024 to achieve those control objectives, if the subservice organizations and user entities applied the complementary controls assumed in the design of Podcastle's controls throughout the period from 1 March 2024 to 31 August 2024. 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 Podcastle,

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 Podcastle's commitments and system requirements,

System was available for operation and use, to achieve Podcastle's commitments and system requirements,

System information is collected, used, disclosed, and retained to achieve Podcastle's commitments and system requirements,

System processing is complete, valid, accurate, timely, and authorized to meet Podcastle's commitments and system requirements,

Personal information is collected, used, retained, disclosed, and disposed to meet Podcastle's commitments and system requirements, based on the Control Criteria.

Podcastle, Inc. Management

28 October 2024

PODCASTLE, Inc. System Description

Podcastle, Inc. Background

Podcastle, Inc., established in 2020, is an information technology company, dedicated to audio and video content creation. It develops the Podcastle suite of AI-driven technologies designed to simplify the entire content production process for companies and individuals. These tools make up a platform with instruments to create quality podcasts and videos with minimal effort with optimization for both the workflow and the product.

The platform features advanced speech and voice manipulation technologies, including **AI-based voice cloning**, **automatic silence removal**, and **AI-generated voices**. These solutions streamline key production processes, such as generating transcripts, cleaning up audio, and creating podcasts using AI. Company provides royalty-free music library and off-line uncompressed audio and video recording capability.

Podcastle, Inc. have its shareholders, as follows:

- Artavazd Yeritsyan,
- Louis Dussart,
- Simon Levegne,
- Ben Yu.

Control Environment

Podcastle, Inc. management have identified the controls over the system throughout the 1 March 2024 to 31 August 2024 to achieve its commitments and system requirements related to the operation using the criteria for 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*. 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 Podcastle's commitments and system requirements,

System is available for operation and use, to achieve Podcastle's commitments and system requirements,

System information is collected, used, disclosed, and retained to achieve Podcastle's commitments and system requirements,

System processing is complete, valid, accurate, timely, and authorized to meet the Podcastle's commitments and system requirements,

Personal information is collected, used, retained, disclosed, and disposed to meet the Podcastle's commitments and system requirements, based on the Control Criteria.

Scope

The scope of the systems covered in this report includes:

The key product of the Company

Podcastle is a platform designed to make long form audio and video content creation and editing accessible and efficient. It provides a suite of tools and features aimed at simplifying the entire Audio and Video content production process, from recording to editing and publishing. Here's an overview of some key aspects of the Podcastle product:

1. **Recording:**
   - **Studio-Quality Recording:** Podcastle offers high-quality audio/video recording capabilities that can be done directly through the platform. Users can record solo or with guests, regardless of their location.
   - **Remote Recording:** It allows for remote recording sessions with multiple participants, making it easy to include guests from different locations.

2. **Editing:**
   - **Simple Editing Tools:** The platform includes user-friendly Audio/video editing tools that cater to both beginners and experienced content creators.
   - **AI-Powered Features:** Podcastle leverages AI to provide advanced editing features such as automatic noise reduction, Studio sound (Magic Dust), voice enhancement, Text to speech and transcription services. These tools help improve audio/video quality and streamline the editing process.

3. **Enhancements:**
   - **Voice Cloning:** The platform offers a voice cloning feature, allowing users to create a digital replica of their voice for various uses in their episodes.
   - **Sound Effects and Music:** Users have access to a library of sound effects and music tracks that can be added to their podcasts to enhance the listening experience.

4. **Publishing:**
   - **Easy Distribution:** Podcastle simplifies the publishing process by enabling users to directly distribute their podcasts to major platforms like Apple Podcasts, Spotify, and other platforms.
   - **SEO Optimization:** The platform provides tools for optimizing podcast descriptions and metadata to improve discoverability.

5. **User Experience:**
   - **User-Friendly Interface:** Podcastle's interface is designed to be intuitive and easy to navigate, making it accessible for users with varying levels of technical expertise.
   - **Collaboration:** The platform supports collaborative work, allowing teams to work together on podcast projects seamlessly.

Overall, Podcastle aims to provide a toolkit for podcasters covering the full life cycle including podcasts creation, editing, and publishing.

The key products of the Company are:

- Podcastle Audio Editor,

- Podcastle Video Editor,

- Podcastle Mobile App,

- Podcastle Recording Studio.

The Key organizational units (teams) of the Company are:

- Infrastructure and Operations department,

- Engineering department,

- Product department,

- Finance department,

- Marketing department,

- Legal department,

- IOS platform unit,

- Dev Ops, System Monitoring and Control unit,

- QA unit,

- Growth unit,

- Video Editor unit,

- Audio Editor and Collaboration unit,

- Recording Studio unit,

- Text Editor unit,

- Administrative unit,

- Customer Support unit,

- Recruitment unit,

- Information security unit.

The key tools of the Company used for product development:

- Google workspace,

- Google Cloud Platform,

- GitHub,

- Kubernetes,

- MongoDB,

- Kibana,

- Elastic Search,

- Testrails,

- Testflight,

- Figma,

- JIRA,

- SonarCloud,

- G-Suite,

- Slack,

- Braze,

- Amplitude,

- Firebase,

- Cloudflare.

IT infrastructure

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

Podcastle, Inc.'s servers are hosted in Google Cloud Platform. Only switch room is located in the Yerevan office, which serves the GPU servers for AI/ML experiments, internal network and enterprise Wi-Fi access points.

Web Protection

To enhance the Company's security posture, Cloudflare's solutions are implemented. Cloudflare offers comprehensive DDoS protection, Web Application Firewall (WAF), and CDN services to protect against various cyber threats and improve the performance and reliability of services.

Website

Podcastle.ai

Locations

The Company locations covered in this report include:

- 9 Isahakyan street, Yerevan, Armenia

Backup Strategy

The Company maintains backups of critical data and configurations in separate environments to mitigate the risk of data loss in case of unforeseen events. The existing backup procedures adhere to industry best practices and are regularly tested for data recovery effectiveness.

Failover Technology

To ensure high availability and fault tolerance, failover technology is implemented. This ensures that the Company services remain accessible even in the event of server or infrastructure failures, minimizing downtime for the end users.

Encryption

The Company uses AES 256 for data "at-rest", TLS 1.2 and TLS 1.3 for data "in-transit".

Vulnerability Management

The Company's vulnerability management approach includes:

- The Company conducts regular vulnerability assessments and penetration tests to identify weaknesses in infrastructure and applications. Identified vulnerabilities are promptly addressed following a risk-based prioritization approach;

- The Company has established processes for applying security patches and updates to mitigate known vulnerabilities in a timely manner;

- Penetration Tests - minimum once per year.

People

Podcastle, Inc.'s organizational structure provides a framework for planning, executing, and controlling business operations. Executive and senior leadership play important roles in establishing Podcastle, 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 dedicated information systems, tools, processes, systems, security practices, policies and procedures. Employees are provided with the set of the Podcastle, Inc.'s policies and pass induction training to educate them as to their responsibilities concerning information security.

Customer Data

Podcastle, Inc. collects the following customer data:

- First and last name,

- Email address,

- Notes,

- Voice recordings,

- Watched content,

- Feature usage,

- Video playlist,

- Usage Data is collected automatically when using the Service. This may include but are not limited to information such as device's IP address, browser type and version, pages visited, time and date of visit, time spent on pages, unique device identifiers, and other diagnostic data. When the client access the Services through a mobile device, the Company may collect certain information automatically, including, but not limited to, the type of mobile device that is used, mobile device unique ID, the IP address of mobile device, mobile operating system, the type of mobile Internet browser that is used, unique device identifiers and other diagnostic data. The Company can also collect information that the client's browser sends whenever they use the Company's Services or when the client accesses the Services through a mobile device,

- Billing Data – while paying for Subscription via payment platforms, such as major credit and debit cards or PayPal, the billing information will be collected by those platforms and shall be governed by the Privacy Policy of those platforms, and the Company shall not have access to this information. However, in cases when automatic payment is not possible for any technical reason, the Company may issue an invoice to receive payment, that in its turn is available for users via their account settings. In such cases the client need to provide billing information, as indicated in the Terms, and the client explicitly provide consent for the Company to use that information for billing purposes,

- Other ID and/or Photo (in specific instances, to comply with GDPR and CCPA compliant requests, the Company may have the need to authenticate customer's account and request to provide an ID and/or photo. This data shall be used solely for the purpose of serving the customer with their requests).

Availability

Podcastle's products are designed in a manner that allows maintaining the availability of its services through defined programs, processes, and procedures. The Business Continuity Program encompasses the processes and procedures by which the Company 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 Podcastle Business Continuity Program is regularly reviewed and approved by the senior leadership.

The Company 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.

Podcastle solutions operate on Google cloud.

Podcastle's backend infrastructure is hosted on GCP, it is fully automated and monitored by continuous functional tests to detect any sort of downtime, protecting infrastructure needs and supporting availability commitments and requirements. Additionally, the Company maintains a capacity planning model to assess infrastructure usage and demands.

Security

The Company has established information security policies and there is an executive-level commitment to implement and comply with the policies throughout the organization.

Information Security function is led by the DPO of Podcastle Inc.

Confidentiality

Podcastle is committed to protecting the security and confidentiality of its customers' content, defined "Privacy Policy" at Privacy Policy | Podcastle. Podcastle communicates its confidentiality commitment to its customers in "Terms and conditions" at Terms & Conditions | Podcastle.

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

Privacy

Podcastle is committed to protecting the personal data of its customers' content, defined as "Privacy Policy" at Privacy Policy | Podcastle. The extent of PII collected and retained by the Company, as well as objectives for PII collection, processing and retention are described in the "Privacy Policy".

Podcastle communicates its privacy commitment to its customers in "Terms and conditions" at Terms & Conditions | Podcastle.

Complementary user entity controls

Podcastle users need to implement and maintain effective internal controls. Each user must evaluate its own internal controls to determine if the following controls and procedures are in place. Podcastle products were designed with the assumption that certain controls would be implemented by user entities. In certain situations, the application of specific controls at user entities is necessary to achieve certain applicable trust services criteria included in this report. This section describes other internal control structure policies and procedures that should be in operation at user entities to complement the control structure policies and procedures at Podcastle:

1. Users are responsible for managing user accounts and permissions for users of their Podcastle Platform solutions,

2. Users are responsible for the accuracy of the data loaded into the Podcastle Platform solutions,

3. Users are responsible for ensuring passwords and other access controls remain unique and confidential,

4. Users are responsible for defining their own data retention policies and utilizing the Podcastle Platform solutions' functionality to remove data per their policy.

Complementary subservice organization controls

Podcastle'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 Podcastle's services to be solely covered by Podcastle's control procedures. Accordingly, subservice organizations, in conjunction with the service, should establish their own internal controls or procedures to complement those of Podcastle, Inc.

Subservice organization controls relevant to the following control criteria should be implemented by AWS and Google workspace to provide additional assurance that the trust services criteria described within this report are met.

Subservice organization	Description
AWS	Cloud hosting services
Google workspace	Cloud hosting services

The following are the applicable trust services criteria and controls that subservice organizations should establish to complement those of PODCASTLE, Inc., provide additional assurance that the Trust Services Criteria described within this report are met.

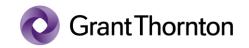| Criteria	Control
CC6 Series **Logical and Physical Access**	- Physical access to the datacenter facilities is restricted to authorized personnel. • Physical access to data centers is approved by an authorized individual. - Procedures are implemented to authenticate authorized users, restrict access and detect unauthorized access attempts. - Security measures are implemented to provision and de-provision user access to systems and applications based on appropriate authorization. - Encryption has been implemented, by default or as configured by the subservice organization, to secure the transmission and storage of information. - Procedures are implemented to securely decommission and physically destroy production assets.
CC7 Series **System Operations**	- Vulnerability scans and penetration testing are performed periodically to identify vulnerabilities threatening the systems.

Criteria	Control
	- Incident response procedures are established and implemented to identify, analyze and remediate events and/or incidents.
	- Environmental protections, monitoring and procedures for regular maintenance are implemented at the datacenter facilities.
CC9 Series **Risk Mitigation**	- Procedures are established and implemented to ensure risk mitigation activities are identified, selected, and developed for risks arising from potential business disruptions.
A Series **Availability**	- Monitoring tools are implemented to monitor and manage the capacity and availability of hosting infrastructure.
	- Environmental protections, data backup processes and recovery mechanisms have been implemented and are appropriately tested to adequately address availability requirements.

Podcastle, Inc.'s management, along with the subservice organizations, defines the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria trough written contracts, such as SLAs. In addition, PODCASTLE performs monitoring of the subservice organization controls, including the following:

- Holding periodic discussions with vendors and subservice organizations,

- Reviewing attestation reports over services provided by vendors and subservice organizations, if applicable.

As described above these processes, activities, and relevant controls are considered as an integral part of Podcastle's operations and control environment and are therefore fully included in the scope of the current examination. These include the following products and business processes:

- software development,

- consulting activities in the field of computer technologies,

- computer systems management activities,

- data processing,

- distribution of information on the network and related activities,

- activities related to web portals.

Grant Thornton

www.grantthornton.am