

## System and Organization Controls (SOC) 3 Report for

# Reprise

For the period October 1, 2021 to March 31, 2022

## Table of Contents

<b>Independent Service Auditor's Report Provided by Laika Compliance LLC</b>	<b>3</b>
<b>Assertion of Reprise Inc.'s Management</b>	<b>5</b>
<b>Attachment A - Reprise Platform Overview</b>	<b>6</b>
<b>Attachment B - Principal Service Commitments and System Requirements</b>	<b>11</b>

# Independent Service Auditor's Report Provided by Laika Compliance LLC

To: Reprise, Inc. ("Reprise" or "the Company")

## Scope

We have examined Reprise's accompanying assertion titled "Assertion of Reprise's Management" (assertion) that the controls within the Company's Reprise Platform (system) were effective throughout the period October 1, 2021 to March 31, 2022, to provide reasonable assurance that Reprise's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Reprise is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Reprise's service commitments and system requirements were achieved. Reprise has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Reprise is responsible for selecting, and identifying in its assertion, the applicable trust service 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 on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

## **Inherent Limitations**

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements 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 that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

## **Opinion**

In our opinion, management's assertion that Reprise's controls over the Reprise Platform were effective throughout the period October 1, 2021 to March 31, 2022, to provide reasonable assurance that Reprise's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

*Laika Compliance LLC*

Arlington, Virginia

June 16, 2022

## Assertion of Reprise Inc.'s Management

We, as management of Reprise Inc., are responsible for:

- Identifying the Reprise Platform (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and system requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion.

Reprise uses a subservice organization for data center colocation services. The boundaries of the System presented in Attachment A includes only the controls of Reprise and excludes controls of the subservice organization. However, the description of the boundaries of the system does present the types of controls Reprise assumes have been implemented, suitably designed, and operating effectively at the subservice organization. Certain trust services criteria can be met only if the subservice organization's controls are suitably designed and operating effectively along with the related controls at Reprise. However, we perform monitoring procedures for the subservice organization and based on procedures performed, nothing has been identified that prevents us from achieving our specified service commitments and system requirements.

We assert that the controls over the system were effective throughout the period October 1, 2021 to March 31, 2022, to provide reasonable assurance that Reprise's service commitments and system requirements would be achieved based on the criteria relevant to Security set forth in the AICPA's TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Reprise, Inc.

## Attachment A - Reprise Platform Overview

### Services Provided

Reprise, Inc. (“Reprise” or “the Company”) is a software as a service company. Reprise offers a software as a service application to provide a demo creation platform used to create and control software demos. Its platform captures screens of the product using the browser, changes text, data, and flow of screens, locks the replay as designed, and makes customized demos, website based product tours, and emailable product experiences that enable businesses to capture, edit, and deploy software product demos based on their existing production application.

The system description in this section of the report details the Reprise Platform. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organization).

### INFRASTRUCTURE

The Company utilizes Google Cloud Platform (GCP) to provide the resources to host the Reprise Platform. The Company leverages the experience and resources of GCP to quickly and securely scale as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the architecture within GCP to ensure security and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure			
Production Tool	Business Function	Operating System	Hosted Location
Reprise API	Provides access to the Reprise SaaS application programming interface	GCP Proprietary	GCP
Cloud Storage	Provides storage of user demo media	Google Cloud SQL	GCP
GCP Container Registry	Stores, manages, and secures Docker container images	GCP Proprietary	GCP

Google Cloud Build	Provides build, test, and deployment services for the serverless CI/CD platform	GCP Proprietary	GCP
Google Cloud CDN	Provides content delivery and workload distribution services	GCP Proprietary	GCP
Google Cloud Storage Buckets (GCS)	Provides media storage services	GCP Proprietary	GCP
Google Kubernetes Engine (GKE)	Provides service networking	GCP Proprietary	GCP
Cloud SQL	Relational database management	GCP Proprietary	GCP
Google Load Balancer	Load balancer	GCP Proprietary	GCP

**SOFTWARE**

Software consists of the programs and software that support the Reprise Platform (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor the Reprise Platform include the following applications, as shown in the table below:

<b>Software</b>	
<b>Production Application</b>	<b>Business Function</b>
Google Cloud IAM	Identity Management
Stackdriver	Infrastructure Logging and Monitoring
Github	Version Control and Source Code Repository
Google Container Registry	Store, Manage and Secure Docker Container Images

Garden	Development, Testing and Troubleshooting
SendGrid	Customer Support and Communication
Tinybird	Data API
Datadog	Application Monitoring
GSuite	Productivity and Collaboration
Slack	Error and Incident Monitoring and Communication
1Password	Password Manager
Electric	IT Support and Asset Management

## PEOPLE

The Company develops, manages, and secures the Reprise Platform via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	Function
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for Reprise Platform.
Operations	Responsible for operations and accounting.
Product	Responsible for overseeing product design and development



The following organization chart reflects the Company's internal structure related to the groups discussed above:

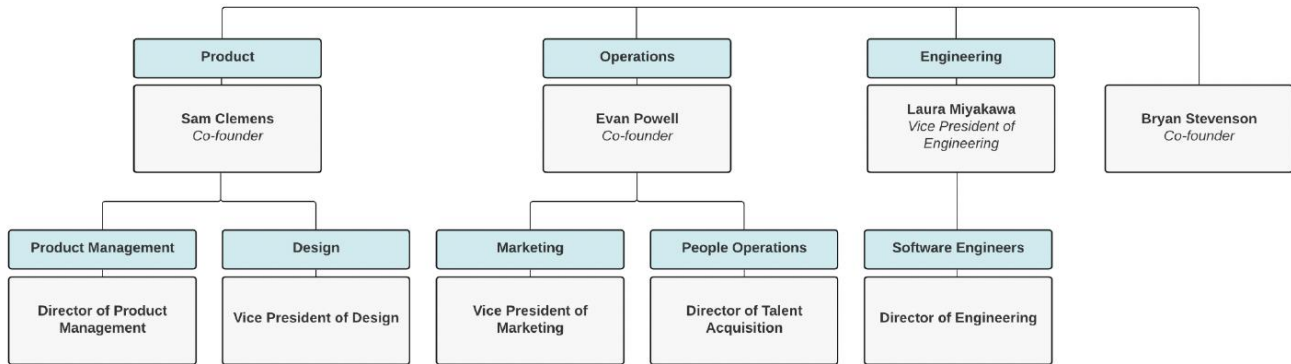


Figure 1: Reprise Organization Chart

## PROCEDURES

Procedures include the automated and manual procedures involved in the operation of the Reprise Platform. Procedures are developed and documented by the respective teams for a variety of processes. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of Reprise Platform:

Procedure	Description
Logical and Physical Access	How the Company restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Change and Configuration Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk and Compliance	How the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Business Continuity and Disaster Recovery (BC/DR)	How the Company identifies the steps to be taken in the event of a disaster to help resume business operations.
---	---

**DATA**

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the Reprise Platform production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Database’s housing sensitive customer data are encrypted at rest.

**COMPLEMENTARY USER ENTITY CONTROLS (CUECs)**

Reprise’s controls were designed with the assumption that certain controls would be implemented by user entities (or “customers”). Certain requirements can be met only if complementary user entity controls assumed in the design of Reprise’s controls are suitably designed and operating effectively, along with related controls at Reprise. Identified complementary user entity controls were included in the service auditor’s examination of SOC 2 controls.

## Attachment B - Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of Reprise Platform. Commitments are communicated in Reprise’s Terms and Conditions (<https://www.getreprise.com/tc/>).

System requirements are specifications regarding how Reprise should function to meet the Company’s principal commitments to user entities. System requirements are specified in the Company’s policies and procedures.

The Company’s principal service commitments and system requirements related to the Reprise Platform include the following:

Trust Services Category	Service Commitments	System Requirements
<p><b>Security</b></p>	<p>Reprise will take reasonable precautions to protect customer data.</p>	<ul style="list-style-type: none"> <li>• Identity and access control</li> <li>• Security monitoring and reporting</li> <li>• Threat management</li> <li>• Security incident response</li> <li>• Security awareness training</li> <li>• Third party provider controls (vendor risk management)</li> <li>• Change control procedures</li> </ul>