Proprietary & Confidential

System Description of the Video Messaging Service

SOC 3
Relevant to Security

Integrated SOC 3 Report Prepared in Accordance with the AICPA Attestation Standards

APRIL 1, 2021 TO MARCH 31, 2022

MOSSADAMS

Table of Contents

I. Independent Service Auditor's Report

Loom
85 2nd Street, Suite 100
San Francisco, CA 94105

To the Management of Loom:

Scope

We have examined Loom, Inc.'s ("Loom") accompanying assertion in Section II titled "Loom's Assertion" (assertion) that the controls within Loom's Video Messaging Service (system) were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that Loom'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*).

Loom uses subservice organization Amazon Web Services (AWS) for services related to server hosting, physical and environmental protection, network management, and disk storage to support the Service. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Loom, to achieve Loom's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Loom's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Loom, to achieve Loom'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 operating effectiveness of such controls.

Service Organization's Responsibilities

Loom 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 Loom's service commitments and system requirements were achieved. Loom has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Loom 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 whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we 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 included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Loom's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Loom's service commitments and system requirements based the applicable trust services criteria

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

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 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 the controls within Loom's Video Messaging Service were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that Loom's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Moss Adams LLP

San Francisco, California
May 19, 2022

II. Loom's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Loom's Video Messaging Service (system) throughout the period April 1, 2021 to March 31, 2022 to provide reasonable assurance that Loom's service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in Section III entitled "Loom's Description of the Boundaries of Its Video Messaging Service" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that Loom'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)*. Loom's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III entitled "Loom's Description of the Boundaries of Its Video Messaging Service".

Loom uses subservice organization Amazon Web Services (AWS) for services related to server hosting, physical and environmental protection, network management, and disk storage to support the Service. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Loom, to achieve Loom's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Loom'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 Loom, to achieve Loom's service commitments and system requirements based on the applicable trust services criteria. The description presents Loom's complementary user entity controls assumed in the design of Loom's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that Loom's service commitments and system requirements were achieved based on the applicable trust services criteria.

III. Loom's Description of the Boundaries of Its Video Messaging Service

A. System Overview

1. Services Provided

COMPANY OVERVIEW

Loom, Inc. ("Loom") is a privately held company founded in 2015 and headquartered in San Francisco, California. With Loom, users can utilize async video messaging in an increasingly globally distributed world. Loom has been adopted by many organizations to empower users to communicate more effectively, wherever they are.

SYSTEM DESCRIPTION

The Loom Video Messaging Service ("Service") is a video messaging tool that allows users to easily record through their camera, microphone, and desktop simultaneously. Loom videos are instantly shareable after recording with the click of a button. The Service allows users to communicate more effectively through video. Loom offerings include different plans for teams, such as Starter, Business, and Enterprise plans, which offer specific feature packages tailored to different organizational needs. Loom for Education is a custom plan designed specifically for the needs of educational institutions.

Within Loom, users join a shared Loom Workspace ("Workspace") in which administrators and creators can invite other team members to allow for recording, watching, and collaborating on videos.

A Loom Workspace includes a Library with the following tabs:

- Videos - All videos recorded by a user and other members that have been made available within the Workspace.
- Folders - All folders created by a user and other members that have been made available within the Workspace.
- Archive - All videos and folders a user has archived.

Within the Videos and Folders tabs, users can apply the following filters to find their content:

- Posted - Filters for all videos and folders that users created and posted. Posting a video makes it available to the team in the Workspace.
- Created by me - Filters for all videos and folders that a user has created, posted, or not posted.

Administrators can set default Workspace privacy settings for videos in the Workspace. Users can change these settings on individual videos:

- Anyone with the link - Videos shared with 'Anyone with the link' can be viewed by anyone who has the link to the video.
- Members of this Workspace - A video set to 'Members of this Workspace' can be viewed by any other members of the Workspace.
- Only people added can access - A video shared to 'Only people added can access' can only be viewed by individuals who are explicitly added.

USER INTERFACES

- Web – This interface can be accessed through any modern web browser. It allows users to view, edit, download, share their videos, and organize their libraries.
- Desktop – The Loom desktop application runs on Windows and Mac OS to allow users to record their camera bubble across any browser or application.
- Chrome Extension – The Loom Chrome Extension allows users to record their camera bubble directly in their Chrome browser. Users can record their full desktop or a specific tab within Chrome.
- Mobile – The Loom mobile application is available for iOS and Android devices. Users can record their screens and camera and access their videos on the go.

2. System Boundaries

The system boundaries for consideration within the scope of this report are the production systems, infrastructure, software, people, procedures, and data within the Service.

While the infrastructure remains the same for all the plans, the scope of this report is restricted to the Business, Enterprise, and Education plans of the Loom Service. The Starter plan is out of scope for this report.

3. Subservice Organizations

Loom uses Amazon Web Services (AWS) for services related to server hosting, physical and environmental protection, network management, and disk storage to support the Service.

This subservice organization is excluded from the scope of this report; the controls it is expected to provide are included in the subsequent section titled *Complementary Subservice Organization Controls*.

4. Infrastructure

The Service is an end-to-end Software-as-a-Service (SaaS) solution. The Service is based on a multi-tenant architecture that applies common and consistent management processes and controls to all customers. The infrastructure has been designed to provide high availability and leverages multiple availability zones for redundancy. These data centers have fully redundant power, networking, and connectivity housed in separate secured facilities. The primary components of the Service are built on top of AWS.

5. Software

The Service operates as a web, desktop, Chrome extension, and mobile application.

Additionally, the following third-party software is used to help manage the Service:

Vendor Software	Function
CloudAMQP	CloudAMQP is a hosted messaging queue solution that automates the entire setup, operation, and scaling of RabbitMQ clusters.
Datadog	Datadog is a monitoring service for cloud-scale applications, providing monitoring of servers, databases, tools, and services through a SaaS-based data analytics platform.
Panther	Panther is a monitoring, alerting, and cloud-scale security analytics platform.
GitHub	GitHub provides hosting for software development version control. GitHub allows code and scripts to be standardized through the software development life cycle, including monitoring, testing, and approving of changes, to maintain quality standards for code development.
Okta	Okta provides secure identity management with single sign-on and multi-factor authentication, helps companies manage and secure user authentication into modern applications, and allows developers to build identity controls into applications, website web services, and devices.
Sentry	Sentry is a self-hosted cloud-based error monitoring tool that helps software teams discover, triage, and prioritize errors in real-time.
Terraform	Terraform is an open-source infrastructure-as-code-software tool to let users define and provision data center infrastructure using a configuration language known as JSON.

6. People

The control framework that supports Loom's organizational environment starts with its senior management team. The following are key roles involved in control implementation and maintenance:

- Co-Founder and Chief Executive Officer (CEO)
- Co-Founder and Chief Technology Officer (CTO)
- Vice President of Engineering
- Director of Talent
- Director of Legal

Responsibility for Loom's information security resides with the Risk and Compliance team. In addition to the overall governance provided by the senior management team, the following teams play a key role in the execution of controls:

- *Engineering*
- *Information Technology (IT)*
- *Infrastructure*
- *Legal*
- *Risk and Compliance*
- *Security*
- *Support*

7. Data

Within the Service, service data is defined as any electronic data, text, videos, transcriptions, comments, communication, or other information submitted by the customer to Loom. Loom also collects customer data which is defined as personally identifiable information such as name, email address upon registration, authentication and payment information (if on a paid plan), and personal data such as IP addresses, hardware and software versions, cookies, etc., from the customer.

8. Processes and Procedures

Loom has developed and communicated to its personnel procedures to protect service data and the company's assets. Procedures are documented and updated on the company intranet to help ensure personnel are informed and equipped to perform their duties to preserve the security of the Service and the service data. These procedures include the following policies:

- Acceptable Use of Technology
- Access and Authorization
- Change Management
- Code of Conduct
- Cryptography
- Data Classification
- Data Handling
- Incident Response Plan
- Information Security
- Network
- Password Protection
- Risk Assessment and Management
- Third-Party Risk Management
- Vulnerability Management

B. Principal Service Commitments and System Requirements

Loom designs its processes and procedures to meet its security objectives. Those objectives are based on the service commitments that Loom makes to user entities and the financial, operational, and compliance requirements that Loom has established for the Service.

Security commitments to user entities and customers, and a description of the Service, are documented and communicated through the Loom Terms of Service published on the website and through customer agreements.

C. Complementary Subservice Organization Controls

Loom's controls related to the Video Messaging Service cover only a portion of overall internal control for each user entity of Loom. It is not feasible for the criteria related to the Video Messaging Service to be achieved solely by Loom. Therefore, each user entity's internal controls must be evaluated in conjunction with Loom's controls, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Complementary Subservice Organization Controls	
1	Access to hosted systems requires users to use a secure method to authenticate.
2	User content is segregated and made viewable only to authorized individuals.
3	Network security mechanisms restrict external access to the production environment.
4	Customer data is encrypted at rest.
5	New user accounts are approved by appropriate individuals prior to being provisioned.
6	User accounts are removed when access is no longer needed.
7	User accounts are reviewed on a regular basis by appropriate personnel.
8	Access modifications to hosted systems are approved by appropriate individuals prior to being provisioned.
9	Access to physical facilities is restricted to authorized users.
10	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.
11	Encrypted communication is required for connections to the production system.
12	Access to hosted data is restricted to appropriate users.
13	Hosted data is protected during transmission through encryption and secure protocols.
14	Antivirus or antimalware solutions are installed to detect or prevent unauthorized or malicious software.
15	System configuration changes are logged and monitored.
16	Vulnerabilities are identified and tracked to resolution.
17	Security events are monitored and evaluated to determine their potential impact.
18	Operations personnel log, monitor, and evaluate incident events identified by monitoring systems.
19	Operations personnel respond to, contain, and remediate incident events, and update stakeholders, as needed.
20	System changes are documented, tested, and approved prior to migration to production.
21	Access to make system changes is restricted to appropriate personnel.

D. Complementary User Entity Controls

Loom's Video Messaging Service was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its Video Messaging Service. In these situations, the application of specific controls at these customer organizations is necessary to achieve certain criteria included in this report.

This section describes additional controls that should be in operation at the customer organizations to complement the controls at Loom. User auditors should consider whether the following controls have been placed in operation by the customers.

Each customer must evaluate its own internal control structure to determine if the identified customer controls are in place. Users are responsible for:

Complementary User Entity Controls	
1	Customers are responsible for implementing controls to ensure that only authorized individuals are granted access.
2	Customers are responsible for implementing controls to ensure access for terminated users is removed timely.
3	Customers are responsible for implementing controls to ensure user accounts and access permissions are periodically reviewed.
4	Customers are responsible for immediately notifying Loom of any actual or suspected information security breaches.

MOSSADAMS