LITMOS US, L.P.

Litmos Platform

SOC 3

System and Organization Controls (SOC) for Service Organizations Report for the period of April 1, 2024 to March 31, 2025

Aprio®
Passionate for what's next®

Report of Independent Service Auditors issued by Aprio LLP

Table of Contents

I. Report of Independent Service Auditor

We have examined Litmos US, L.P.'s (the "Company" or "Litmos") accompanying assertion titled *Litmos US, L.P.'s Assertion* (the "Assertion") indicating that the controls within the Litmos Platform (the "System") were effective for the period of April 1, 2024 to March 31, 2025 (the "Specified Period") to provide reasonable assurance that Litmos' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (With Revised Points of Focus – 2022) (AICPA, *Trust Services Criteria*) for the Specified Period.

The Company uses Amazon Web Services' (AWS), a subservice organization, Elastic Compute Cloud (Amazon EC2) services for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. The Company also uses the Amazon Relational Database Service as a Database-as-a-Service. In addition, the Company uses Microsoft Azure's (Azure), a subservice organization, Platform-as-a-Service for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. The Company also uses the Office 365 / OneDrive and Microsoft Entra ID Software-as-a-Service. Further, the Company uses Auxis, a subservice organization, as a managed IT services provider for user access provisioning and deprovisioning, database management, network and firewall management, backup management, infrastructure monitoring and incident response, vulnerability management services, and business continuity and disaster recovery testing services. Certain AICPA applicable trust services criteria specified in the section titled *Litmos US, L.P.'s Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's Assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations. The Assertion 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 organization controls.

Service Organization's responsibilities

The Company 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 the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled *Litmos US, L.P.'s Assertion* about the suitability of design and operating effectiveness of controls. When preparing its assertion, the Company 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 the 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. 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.

We are required to be independent and to meet our ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- obtaining an understanding of the system and the service organization's service commitments and system requirements;
- assessing the risks that the controls were not effective to achieve the Company'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 the Company's service commitments and system requirements based on the applicable trust services criteria;
- performing procedures to obtain evidence about whether controls were suitably designed and operating effectively to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- testing the operating effectiveness of controls to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on 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.

Other matters

We did not perform any procedures and accordingly do not express an opinion on the description in Section III titled *Litmos US, L.P.'s Description of the Boundaries of its System*.

Opinion

In our opinion, Litmos' assertion that the controls within the Company's System were effective throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, in all material respects, is fairly stated.

Aprio, LLP

Aprio, LLP

Atlanta, Georgia
May 15, 2025

II. Litmos US, L.P.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over Litmos US, L.P.'s (the "Company" or "Litmos") Litmos Platform (the "System") for the period of April 1, 2024 to March 31, 2025 (the "Specified Period"), to provide reasonable assurance that the Company's service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. We have performed an evaluation of the effectiveness of the controls within the System throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (the "applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (With Revised Points of Focus – 2022) (AICPA, *Trust Services Criteria*). The Company'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. Our description of the boundaries of the system and principal service commitments and system requirements related to the applicable trust services criteria are specified in the section titled *Litmos US, L.P.'s Description of the Boundaries of its System*.

The Company uses Amazon Web Services' (AWS), a subservice organization, Elastic Compute Cloud (Amazon EC2) services for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. The Company also uses the Amazon Relational Database Service as a Database-as-a-Service. In addition, the Company uses Microsoft Azure's (Azure), a subservice organization, Platform-as-a-Service for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. The Company also uses the Office 365 / OneDrive and Microsoft Entra ID Software-as-a-Service. Further, the Company uses Auxis, a subservice organization, as a managed IT services provider for user access provisioning and deprovisioning, database management, network and firewall management, backup management, infrastructure monitoring, incident response, vulnerability management services, and business continuity and disaster recovery testing services. Certain AICPA applicable trust services criteria specified in the section titled *Litmos US, L.P.'s Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations.

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 Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria.

III. Litmos US, L.P.'s Description of the Boundaries of its System

A. Scope and Purpose of the Report

This report describes the control structure of Litmos US, L.P. (the "Company" or "Litmos") as it relates to its Litmos Platform (the "System") for the period of April 1, 2024 to March 31, 2025 (the "Specified Period"), for the trust services criteria relevant to Security, Availability, and Confidentiality (the "Applicable Trust Services Criteria") as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (With Revised Points of Focus – 2022) (AICPA, *Trust Services Criteria*).

It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. The internal control structures at the Company are not designed to compensate for any weaknesses that may exist if the internal control structure at a user organization is ineffective.

B. Company Overview and Background

Litmos develops online learning solutions and offers an easy-to-use Learning Management System (LMS) with a comprehensive learning content library. Thousands of companies rely on Litmos LMS to create, curate, and connect learning content to employees, customers, and partners.

Acquired by CallidusCloud in 2011, then by SAP in 2018, and by Francisco Partners in 2022, Litmos continues to innovate learning technology for customer experience and satisfaction. The solutions are used by more than 30 million people in 150 countries and across 35 languages.

Litmos Platform Overview

Through a Software-as-a-Service (SaaS) delivery model, the Litmos platform provides the capabilities of Litmos's software to customers via the Internet. The LMS offering includes the delivery of software, the installation of updated versions, and the provision of technical support backed by a Service Level Agreement which includes a 99.5% uptime guarantee for production sites. Litmos's customers can choose localized hosting within the US, EU, or Australia. Main features of the LMS and services provided include the AI Assistant, AI/ML Video Assessments, AI Playlist, Content Authoring Tool, external training, gamification, Instructor Led training, Learning Engagement, Manager Insights, mobile learning and reporting and analytics. The Litmos LMS SaaS product is multi-tenant.

C. System Overview

Supporting Systems Overview

The Litmos LMS is a web-based resource which provides Litmos customers with access to tools and information. LMS users can obtain support and tips from the Litmos Customer Support team, watch product webinars, register for training, view the latest software documentation, and more.

1. Infrastructure and Databases

Litmos has key operations and cloud data centers in the following locations supporting Litmos:

- Frankfurt, Germany – Amazon Web Services (eu-central-1)
- Frankfurt, Germany – Microsoft Azure (Germany West Central)
- Frankfurt, Germany – Google Cloud Platform (Europe-west3)
- Sydney, Australia – Amazon Web Services (ap-southeast-2)
- New South Wales, Australia – Microsoft Azure (Australia East)

- Sydney, Australia – Google Cloud Platform (australia-southeast1)
- Virginia, USA – Amazon Web Services (us-east-1)
- Virginia, USA – Microsoft Azure (US East)
- N. Virginia, USA – Google Cloud Platform (us-east4)
- California, USA – Microsoft Azure (West US)

The AWS and Azure infrastructure have been designed to provide a reliable and highly available platform. The key services provided by these cloud service providers include hyperscaling so that underlying equipment redundancy is in place to help ensure the availability of the provisioned services. Firewall services are implemented for the virtual network perimeter to filter incoming and outgoing traffic. Litmos manages MS SQL (Standard Query Language) Server databases for the application but utilizes AWS RDS for a sub-system component.

System Overview	Purpose
Microsoft Azure	System Infrastructure
Amazon Web Services	System Infrastructure
Microsoft SQL Server	Database
AWS RDS	Database
Windows	Operating System
Linux	Operating System
Microsoft Entra ID	Identity and Access Management (IAM) tool

D. Principal Service Commitments and System Requirements

Litmos makes service commitments to its customers, has established systems requirements, and is responsible for designing, implementing, and operating effective controls within the system to provide reasonable assurance that these service commitments and system requirements are achieved.

Litmos's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality. These commitments include, but are not limited to the following:

1. Litmos' security commitments are related to securing service offerings and customer data and complying with relevant laws and regulations. These commitments are addressed through adherence to Litmos security polices and operating practices and measures, including data encryption, authentication mechanisms, incident management, and other relevant security controls.
2. Litmos' availability commitments are related to contractually agreed-upon percentage system uptime and connectivity for services, customer support with committed response times based on the severity of the problem, availability response planning and notification procedures, and continuity and recovery mechanisms to minimize data loss and help to ensure return to operations.
3. Litmos' confidentiality commitments are related to maintaining the confidentiality of customers' data through data classification and record retention policies, data encryption, and restriction of logical access. Customer data hosted utilizing cloud services is deleted in accordance with requirements outlined in customer contracts unless applicable law requires retention.

Operational requirements to support the achievement of security, availability, and confidentiality commitments, as well as compliance with relevant laws, regulations, and other system requirements, are established through policies and procedures documented and communicated internally to relevant stakeholders.

E. Non-Applicable Trust Services Criteria

Security, Availability, and Confidentiality Trust Services Categories		
Non-Applicable Trust Services Criteria		**Litmos's Rationale**
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	N/A – Litmos' hosting providers, Amazon Web Services (AWS) and Microsoft Azure, are responsible for physical security controls. Litmos does not maintain any hard copy data or store any customer information physically.

F. Subservice Organizations

The Company utilizes a subservice organization to perform certain functions. The description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party subservice organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organizations and are necessary to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organizations. Each user entity's internal control must be evaluated in conjunction with the Company's controls and taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Amazon Web Services	Litmos uses Amazon AWS Elastic Compute Cloud (Amazon EC2) services for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. Litmos also uses the Amazon Relational Database Service (Amazon RDS) as a Platform-as-a-Service, more specifically a Database-as-a-Service. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure and Data Centers supporting the in-scope production environments including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing infrastructure security such as physical servers and physical access to backups and facilities; • Controls over the change management processes for the physical servers supporting the Infrastructure-as-a-Service Platform;	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• Controls over the configuration settings within the EC2 instance to ensure that data is encrypted and stored as per the configuration settings selected with AWS; • Controls over incident monitoring, response, and follow up; • Controls over managing the Platform-as-a-Service components for (Amazon RDS) such as physical servers and operating systems including applying critical patching for this infrastructure; • Controls over Amazon RDS including operating system installation and patches; database software installation and patches; and routers/firewalls monitoring and maintenances; and • Controls over the change management processes for the AWS Infrastructure-as-a-Service Platform and the Platform-as-a-Service Platform (RDS) components as applicable. In addition, Litmos has identified the following control activity to help monitor the subservice organization: • On an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the system and either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls annually, based off the vendor contract signing date. Corrective actions are taken, if necessary.	A 1.1* A 1.2* A 1.3* C 1.1* C 1.2*
Microsoft Azure	Litmos uses Microsoft Azure's Platform-as-a-Service for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. Litmos also uses the Office 365 / OneDrive and Microsoft Entra ID and Microsoft (MS) Defender as a Software-as-a-Service. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure and Data Centers supporting the in-scope production environments including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing the security of infrastructure and software such as physical servers and physical access to backups and facilities; • Controls over the change management processes for the software and infrastructure supporting the platform; • Controls over incident monitoring, response, and follow up; • Controls over the prevention, detection, and follow up upon the introduction of malicious software; • Controls over Azure Storage redundancy, including controls over data replication; • Controls over the monitoring of the Office 365 / OneDrive, Microsoft Entra ID, and Microsoft Defender Software-as-a-Service components including backups, anti-virus, and incidents	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2* A 1.1* A 1.2* A 1.3*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	related to security and availability including responding to items identified; • Controls over the encryption of transmitted and stored data within the platform; and • Controls over managing patching for the software and infrastructure supporting the platform. In addition, Litmos has identified the following control activity to help monitor the subservice organization: • On an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the system and either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls annually, based off the vendor contract signing date. Corrective actions are taken, if necessary.	C 1.1* C 1.2*
Auxis	Litmos uses Auxis as a managed IT services provider for user access provisioning and deprovisioning, database management, network and firewall management, backup management, infrastructure monitoring and incident response, vulnerability management services, and business continuity and disaster recovery testing services. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over incident monitoring, response, and follow up for the network, databases, and underlying infrastructure supporting the Litmos Platform; • Controls over the change management processes for the databases and infrastructure supporting the in-scope production environments; • Controls over restricting logical access to the network, databases, and underlying infrastructure supporting the Litmos Platform; • Controls over the encryption of transmitted and stored data within the databases; • Controls over the management of network firewalls and security groups for in-scope production databases; and • Controls over the availability of in-scope production databases, including failover testing. In addition, Litmos has identified the following control activity to help monitor the subservice organization: • On an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the system and either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls annually, based	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.5* CC 8.1* CC 9.1* CC 9.2* A 1.1* A 1.2* A 1.3* C 1.1* C 1.2*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	off the vendor contract signing date. Corrective actions are taken, if necessary.	

** The achievement of design and operating effectiveness related to this criterion assumes that the complementary controls at this subservice organization that support the service organization's service commitments and system requirements are in place and are operating effectively.*

G. User Entity Responsibilities

Each user entity must evaluate its own system of internal controls for effective risk management and compliance. The internal controls described in this report occur at and are managed by the Company and only cover a portion of a comprehensive internal control structure relevant to a user entity. Each user entity must address the various aspects of internal control that may be unique to its particular organization. This section highlights those portions of the internal control structure that user entities have responsibility to develop and maintain but should not affect the ability of the Company to achieve its service commitments and system requirements.

Related Control Area	User Entity Responsibilities
Monitoring & Communication	• Customers are responsible for communicating relevant security, availability, and confidentiality issues and incidents to Litmos through identified channels. • Customers are responsible for notifying Litmos of any unauthorized use of any password or account or any other known or suspected breach of security related to the Litmos LMS or Litmos Training Ops platforms.
Access	• Customers are responsible for helping to ensure that authorized users are appointed as organizational administrators for granting access to Litmos LMS or Litmos Training Ops platforms. • Customers are responsible for restricting logical access to in-scope applications, including addition and removal of access. • Where applicable, Customers are responsible for granting and removing access for Litmos customer support personnel and defining an appropriate expiration date when granting access.
Policies & Procedures	• Customers are responsible for configuring the data retention settings within the Litmos LMS and Litmos Training Ops platforms. • Customers are responsible for data classification and the implementation of encryption features available (where applicable) within Litmos LMS or Litmos Training Ops platforms, where deemed necessary by the defined User Entities' requirements.


Aprio