Report on Riverbed Technology LLC's Alluvio IQ Platform Relevant to Security and Availability Throughout the Period July 1, 2022 to September 30, 2022

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Section 2

Attachment A

Attachment B

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Riverbed Technology LLC ("Riverbed")

Scope

We have examined Riverbed's accompanying assertion titled "Assertion of Riverbed Technology LLC Management" (assertion) that the controls within Riverbed's Alluvio IQ Platform (system) were effective throughout the period July 1, 2022 to September 30, 2022, to provide reasonable assurance that Riverbed's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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*).

Service Organization's Responsibilities

Riverbed 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 Riverbed's service commitments and system requirements were achieved. Riverbed has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Riverbed 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, based on our examination, on 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. 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 Riverbed'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 Riverbed's 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.

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

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 Riverbed’s Alluvio IQ Platform were effective throughout the period July 1, 2022 to September 30, 2022, to provide reasonable assurance that Riverbed’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
November 29, 2022

Section 2

Assertion of Riverbed Technology LLC Management

Assertion of Riverbed Technology LLC (“Riverbed”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within Riverbed’s Alluvio IQ Platform (system) throughout the period July 1, 2022 to September 30, 2022, to provide reasonable assurance that Riverbed’s service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented in attachment A 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 July 1, 2022 to September 30, 2022, to provide reasonable assurance that Riverbed’s service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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*). Riverbed’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 attachment B.

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 July 1, 2022 to September 30, 2022 to provide reasonable assurance that Riverbed’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Riverbed Technology LLC

Attachment A

Riverbed Technology LLC’s Description of the Boundaries of Its Alluvio IQ Platform

Type of Services Provided

Riverbed Technology LLC’s (“Riverbed” or “Company”) Alluvio IQ platform is a cloud-native, software-as-a-service (SaaS)-delivered, open, and programmable solution for unified observability that empowers all information technology (IT) staff to identify and fix problems fast. It uses full-fidelity end user experience and network performance data across every transaction in the digital enterprise and then applies artificial intelligence (AI) and machine learning (ML) to contextually correlate data streams and alerts to identify the most business impacting events. This intelligence also informs investigative runbooks that replicate the troubleshooting workflows of IT experts to gather added context, filter out noise, and set priorities — reducing the volume of alerts to the most business impacting and empowering staff at all skill levels to identify and solve problems fast.

The Components of the System Used to Provide the Services

The boundaries of Alluvio IQ are the specific aspects of the Company’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of Alluvio IQ.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The Company utilizes a third-party cloud service provider to provide the resources to host Alluvio IQ. The Company leverages the experience and resources of the cloud service provider to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the Alluvio IQ architecture within the third-party cloud service provider to ensure the availability, security, and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools to address the following business functions:

- Customer data ingestion and transformation
- Customer data storage
- Distribution of static web application user interface (UI) assets

Software

Software consists of the programs and software that support Alluvio IQ (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor Alluvio IQ include applications to support the following business functions:

- Application monitoring
- Backup and replication
- Security information and event management (SIEM), logging system
- Infrastructure monitoring

- Patch management
- Antivirus
- Intrusion detection and prevention
- Help desk, ticketing system

People

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

People	
Group/Role Name	**Function**
Executive Leadership	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Engineering (including DevOps)	Responsible for the development, testing, deployment, and maintenance of new code for Alluvio IQ.
Information Security (InfoSec)	Responsible for managing access controls and the security of the production environment.
Product Management	Responsible for overseeing the product life cycle, including adding new product functionality.
Human Resources (HR)	Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks, and facilitating the employee termination process.

Procedures

Procedures include the automated and manual procedures involved in the operation of Alluvio IQ. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, IT, and HR. 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 Alluvio IQ:

Procedures	
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 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.

Procedures	
Procedure	**Description**
Risk Mitigation	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the web application user interface (Web UI), the customer or end-user defines and controls the data they load into and store in the Alluvio IQ 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. Databases housing sensitive customer data are encrypted at rest.

Subservice Organization

The Company uses a subservice organization for data center colocation services. The Company's controls related to Alluvio IQ cover only a portion of the overall internal control for each user entity of Alluvio IQ. The description does not extend to the colocation services for IT infrastructure provided by the subservice organization.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. Controls are expected to be in place at the subservice organization related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. The subservice organization's physical security controls should mitigate the risk of unauthorized access to the hosting facilities. The subservice organization's environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

The Company management receives and reviews the subservice organization's SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by the subservice organization to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to management of the subservice organization.

Complementary User Entity Controls

Complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Riverbed, to achieve Riverbed's service commitments and system requirements based on the applicable trust services criteria.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of Alluvio IQ. Commitments are communicated in service-level agreements, the Data Processing Addendum, and the End User License Agreement.

System requirements are specifications regarding how Alluvio IQ 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 Alluvio IQ include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Riverbed has implemented information security policies to establish and enforce Riverbed's corporate security program. • Riverbed has implemented and will maintain encryption of sensitive data. • Riverbed has implemented and will maintain technical and organizational measures to protect the security of sensitive data. • Riverbed will respond, investigate, and remediate security issues when they are detected and will notify the customer without undue delay in the event of a data breach.	• Logical access standards • Employee provisioning and deprovisioning standards • Access reviews • Encryption standards • Intrusion detection and prevention standards • Risk and vulnerability management standards • Configuration management standards • Incident handling standards • Change management standards • Vendor management
Availability	• Riverbed will ensure a production system uptime of 99.5%. • Riverbed will employ measures to ensure the ability to restore the availability and access to sensitive data in a timely manner in the event of a physical or technical incident.	• System monitoring and logging • Backup and recovery standards