APPIAN CORPORATION

Appian Cloud

System and Organization Controls for Service Organizations: Trust Services Criteria for General Use Report (SOC 3) for the period of October 1, 2020 to September 30, 2021
## Contents

I. Report of Independent Service Auditors ................................................................. 1  
II. Assertion of Appian Corporation’s Management ..................................................... 3  

Attachment A - Description of the Boundaries of Appian Corporation’s Appian Cloud System ................................................................................................................. 4  

Attachment B - Principal Service Commitments and System Requirements ............... 8  

I. Report of Independent Service Auditors

Board of Directors and Management
Appian Corporation

Scope
We have examined Appian Corporation’s (“Appian”) accompanying assertion titled Assertion of Appian Corporation’s Management (“assertion”) that the controls within its Appian Cloud System (“system”) were effective throughout the period October 1, 2020 to September 30, 2021, to provide reasonable assurance that Appian’s 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 (AICPA, Trust Services Criteria).

Service organization’s responsibilities
Appian 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 Appian’s service commitments and system requirements were achieved. Appian has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Appian 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 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. 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 Appian’s service commitments and system requirements based on the applicable trust services criteria; and
• Performing procedures to obtain evidence about whether controls within the system were effective to achieve Appian’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 Appian Corporation's Appian Cloud System were effective throughout the period October 1, 2020 to September 30, 2021, to provide reasonable assurance that Appian Corporation's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Kansas City, Missouri
December 6, 2021
II. Assertion of Appian Corporation’s Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Appian Corporation’s (“Appian”) Appian Cloud System (“system”) throughout the period October 1, 2020 to September 30, 2021, to provide reasonable assurance that Appian’s service commitments and system requirements relevant to security, availability, and confidentiality 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 October 1, 2020 to September 30, 2021, to provide reasonable assurance that Appian’s 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 (AICPA, Trust Services Criteria). Appian’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 October 1, 2020 to September 30, 2021, to provide reasonable assurance that Appian’s service commitments and system requirements were achieved based on the applicable trust services criteria.
Attachment A - Description of the Boundaries of Appian Corporation’s Appian Cloud System

Overview of Appian

Company Overview

Appian Corporation ("Appian" or the "Company") was founded on the belief that talented and passionate people, given the power and autonomy to excel, will deliver amazing results. Appian provides a low-code development platform that accelerates the creation of high-impact business applications.

Today, we help customers build apps and workflows rapidly, with a low-code automation platform. We combine people, technologies, and data in a single workflow to maximize customer's resources and dramatically improve business results.

Appian Cloud Overview

Appian helps organizations build apps and workflows rapidly, with a low-code platform. Combining people, technologies, and data in a single workflow, Appian can help companies maximize their resources and improve business results. Appian Cloud provides customers with access to the Appian platform as a hosted Platform as a Service (PaaS).

Components of the System Used to Provide the Services

1. Appian Cloud Infrastructure

   The Appian Cloud infrastructure supports the delivery of the Appian platform for use by customers and is built and hosted within Amazon Web Services (AWS).

   Each Appian Cloud customer site is isolated using separate AWS EC2 instances, and contains the following components dedicated to the customer including:

   • Application Server,
   • Appian Engines, and
   • Database.

   Common infrastructure / services also exist to support all Appian Cloud sites (e.g. DNS, NTP, Syslog, IDS, email, etc.)
2. **Software**

Appian Cloud utilizes several software platforms to operate. A site consists of an instance of Tomcat, the Appian engines, and a MySQL/MariaDB database with phpMyAdmin for customer interaction.

3. **People**

Management instills a philosophy which enables all employees to share in the successes and ultimate growth of the Company. The organization’s management team is comprised of a skilled and diverse group, ultimately responsible for the vision and direction of Appian. These individuals meet regularly to discuss a wide range of topics and are also responsible for establishing corporate policy and addressing all operational, technical, financial, cultural, and social aspects of Appian. Management reviews the Company’s organizational structure as part of strategic planning, and any changes are made as needed based on changing reporting lines, authorities, and responsibilities. The Company’s organizational chart is available to internal users on the Company’s intranet site.
The following is a functional structure of the Appian Chief Information Officer Department:

The internal teams have been established to provide support and quality control for the various operations of Appian Cloud. Each team has a leader who reports to the Chief Information Officer.

Responsibilities and requirements are defined for key job positions, specifically for personnel responsible for the design, development, implementation, and operation of systems affecting Appian Cloud.

The Company’s Code of Business Ethics and Conduct, and security policies and practices are documented and communicated to employees.

4. Data

Each customer’s Appian Low-code Automation Platform is configured so that each customer’s data is isolated from other customers within the Appian Cloud infrastructure; therefore, customers cannot access any data other than their own. All Appian customer environments operate within the Appian Cloud infrastructure production network and have the same production-level controls in place.

Appian maintains strict policies in regard to access to customer information as well as policies about disclosure of customer information. Information security policies define what is confidential information as well as requirements for retention and removal.

5. Processes and Procedures

Appian has documented policies and standard operating procedures which address controls related to system security, availability, and confidentiality for Appian Cloud. These policies and procedures are available to all Appian employees supporting Appian Cloud. Personnel take an Appian Cloud-specific security awareness training which incorporates training information related to the security, availability, and confidentiality obligations of Appian Cloud information. Management reviews these policies and procedures on a periodic basis.

6. Subservice Organization

Appian uses Amazon Web Services 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 firewalls, routers, and servers.

Our description of the boundaries of the system and the principal service commitments and system requirements related to the applicable trust services criteria do not include the services provided by the subservice organization.

Our conclusion regarding effectiveness of controls within the system to achieve Appian’s service commitments and system requirements based on the applicable trust services criteria assumes that the complementary subservice organization controls assumed in the design of Appian’s Cloud system operated effectively throughout the period October 1, 2020 to September 30, 2021.
7. **Complementary User Entity Controls**

   Our description of the boundaries of the system and the principal service commitments and system requirements related to the applicable trust services criteria do not include complementary user entity controls.

   Our conclusion regarding the effectiveness of controls within the system to achieve Appian's service commitments and system requirements based on the applicable trust services criteria assumes that complementary user entity controls assumed in the design of the Appian's controls operated effectively throughout the period October 1, 2020 to September 30, 2021.
Attachment B - Principal Service Commitments and System Requirements

Appian Corporation designs its processes and procedures related to Appian Cloud to meet its objectives for its cloud services. Those objectives are based on the service commitments that Appian makes to user entities, the laws and regulations that govern the provision of Appian Cloud services, and the financial, operational, and compliance requirements that Appian has established for the services. Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security, availability, and confidentiality commitments are standardized and include, but are not limited to, the following:

- Security and confidentiality principles that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role;
- Use of encryption technologies to protect customer data in transit over untrusted networks;
- Availability principles that are designed to help ensure availability of the systems supporting Appian Cloud.

Appian establishes operational requirements that support the achievement of security, availability, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Appian’s system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data is protected.