APPIAN CORPORATION

Appian Cloud

System and Organizational Controls (SOC) for Service Organizations Report
for the period of July 1, 2018 to June 30, 2019

Report of Independent Service Auditors issued by
Grant Thornton LLP

Contents

GRANT THORNTON LLP
1100 Peachtree St NE, Suite 1200
Atlanta, GA 30309

D +1 404 330 2000
F +1 404 330 2047

I. Report of Independent Service Auditors

Board of Directors and Management
Appian Corporation

Scope

We have examined Appian Corporation's (the "Company" or "Appian") accompanying assertion titled *Appian Corporation's Assertion* (the "Assertion") that the controls within Appian Corporation's Appian Cloud (the "System") were effective throughout the period July 1, 2018 to June 30, 2019 (the "specified period"), 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 (the "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*).

The Company uses a subservice organization, Amazon Web Services (AWS), for the hosting of its System's infrastructure. Management's assertion indicates that its assertion and its description in Section III includes only the controls of the Company and excludes the controls of this subservice organization. Management's assertion indicates that certain AICPA Applicable Trust Services Criteria specified by management in Section III, *Appian Corporation'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 the related controls at the Company. Our examination did not extend to the controls of this subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organizations controls.

Management's assertion indicates that certain AICPA Applicable Trust Services Criteria specified in Section III, *Appian Corporation's Description of the Boundaries of its System*, under the section *User Entity Controls*, can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

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 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. 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 System were effective throughout the period July 1, 2018 to June 30, 2019, to provide reasonable assurance that Appian's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria is fairly stated, in all material respects.

Grant Thornton LLP

Atlanta, Georgia
July 1, 2019

II. Appian Corporation's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Appian Corporation's (the "Company" or "Appian") Appian Cloud (the "System") throughout the period July 1, 2018 to June 30, 2019 (the "specified period"), 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 *Appian Corporation's Description of the Boundaries of its System* 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, 2018 to June 30, 2019, 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* (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 *Appian Corporation's Description of the Boundaries of its System*.

The Company uses a subservice organization, Amazon Web Services (AWS), for the hosting of its System's infrastructure. Certain AICPA Applicable Trust Services Criteria, specified in Section III, *Appian Corporation's Description of the Boundaries of its System*, under the section *Subservice Organizations* can be achieved only if complementary subservice organization controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion and the related description of the boundaries of the system in Section III of this report includes only the controls of the Company and excludes the controls performed by this subservice organization.

Certain AICPA Applicable Trust Services Criteria, specified in Section III, *Appian Corporation's Description of the Boundaries of its System*, under the section *User Entity Controls* can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion and the related description of the boundaries of its System in Section III of this report includes only the controls of the Company and excludes the controls performed by User Entities.

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, 2018 to June 30, 2019, to provide reasonable assurance that Appian Corporation's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria.

III. Appian Corporation's Description of the Boundaries of its System

A. Scope and Purpose of the Report

This report describes the control structure of Appian Corporation (the "Company" or "Appian") as it relates to Appian Cloud (the "System") for the period of July 1, 2018 to June 30, 2019 (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* (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. Overview of Services Provided

1. Company Overview

Appian provides a low-code development platform that accelerates the creation of high-impact business applications. Many of the world's largest organizations use Appian's applications to improve customer experience, achieve operational excellence, and simplify global risk management and compliance.

2. Appian Cloud Overview

Through a Platform-as–a-Service delivery model, Appian Cloud provides the capabilities of Appian's software to customers via the Internet. The Appian Cloud offering includes the delivery of the software, the installation of updated versions, and the providing of technical support backed by a Service Level Agreement which includes a 99.95% uptime guarantee for production sites. Appian's customers can choose localized hosting within North America (including the U.S.[1]), EU, Asia Pacific, and South America.

3. Infrastructure

At a high level, there are five major customer-dedicated components in an Appian Cloud site:

- Application Server,
- Appian Engine,
- Database,
- Operating System, and
- AWS EC2[2] Instance.

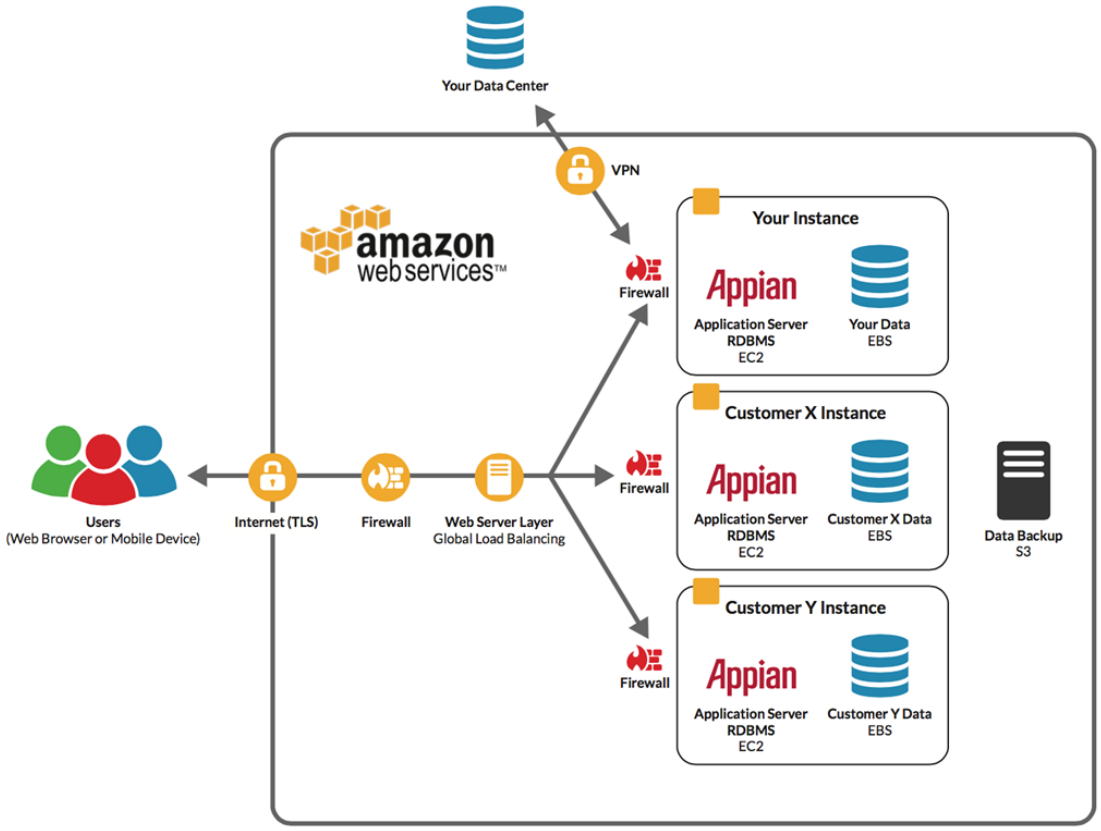
The following exist in the AWS environment to support Appian Cloud sites:

- Web server(s),
- LDAP server(s) which is/are used for user account management across all Linux servers in the environment,

[1] Includes AWS GovCloud
[2] Appian utilizes Amazon Web Services (AWS) as the hosting provider for Appian Cloud.

- Radius server(s) which is/are used for user account authentication across all Linux servers and supports multi-factor authentication using OATH-HOTP,
- Syslog/ossec server(s) which is/are used for centralized logging and host-based IDS,
- Outbound e-mail server(s) which is/are used to relay all outbound e-mails,
- Inbound e-mail server(s),
- Monitoring, and
- Appian Cloud Business Process Management.

The diagram below depicts the Appian Cloud system boundaries:



4. Software

Appian Cloud utilizes several software platforms to operate. A site consists of an instance of JBoss, the Appian engines, a MySQL database, and an instance of Apache web server running phpMyAdmin.

C. Principal Service Commitments and System Requirements

Overview

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.

Non-applicable trust services criteria

Common Criteria (CC)		
Non-Applicable Trust Services Criteria		**Appian Corporation's Rationale**
CC6.4	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 – Appian's hosting provider, Amazon Web Services (AWS), is responsible for physical security controls.

Subservice Organizations

The Company utilizes subservice organizations to perform certain functions. The SOC 3 examination 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 service 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 organization 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 organization. Each user entity's internal control must be evaluated in conjunction with the Company's controls, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Subservice Organization	Services Provided	Associated Criteria
Amazon Web Services	The Company 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. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls around the physical security of the Data Centers hosting the in-scope application; • Controls around the Amazon EBS Snapshot service, including controls around physical access to the backup servers, environmental controls, and the availability of the backup servers; and • Controls around the change management processes for the physical servers and the features offered as part of the AWS Infrastructure-as-a-Service Platform. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On an annual basis, Appian evaluates the third parties who have access to confidential data or perform a managed service related to the operation of the System and determines their risk based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this, Appian performs a vendor security assessment of the third party through methods such as site assessments, security questionnaires, reviews of the third party's System and Organization Control reports such as SOC 2 reports, etc. Corrective actions are taken, if necessary, based on the results of these reviews.	CC6.4 - 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. CC8.1* - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. A1.1* - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

Subservice Organization	Services Provided	Associated Criteria
		A1.2* - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

* The achievement of design and operating effectiveness related to this particular Trust Services Criterion assumes that complementary controls at this subservice organization that support this criterion are in place and are operating effectively.

User Entity Controls

Appian's controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company's service commitments and system requirements to be achieved based on the applicable trust services criteria solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related testing detailed in Section IV of this report, taking into account the related complementary user entity controls identified within the table below, where applicable. Complementary user entity controls and their associated criteria are included within the table below.

Management has highlighted criterion in which complementary user entity controls were assumed in the design of the Company's system with an asterisk. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control environment to determine if the identified complementary user entity controls have been implemented and are operating effectively.

Furthermore, the table below includes suggested control considerations that the Company believes each user organization should consider in developing their internal controls or planning their audits that are relevant to the Company's controls detailed in this report, however, such control considerations are not required to achieve design or operating effectiveness for the Company's service commitments and system requirements based on the applicable trust services criteria. The following list of suggested control activities is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user entity. Accordingly, this list does not allege to be, and is not, a complete listing of all the control activities which provide a basis for the assertions underlying the control environments for the Company's user entities.

User Entity Control	Associated Criteria
Customers are responsible for requesting the description of Appian Cloud.	CC2.3* - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.
Customers are responsible for providing training to users of the application(s) built on Appian Cloud.	CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

User Entity Control	Associated Criteria
	CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
Customers are responsible for reviewing release notes and for notifying Appian of any issues they foresee with the proposed release, including any changes that may affect system security, availability, and/or confidentiality.	CC 5.2* - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
	CC8.1* - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for controlling who has access to their data and for alerting Appian of any unauthorized access and/or issues/breaches.	CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
	CC6.1* - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	CC6.6* - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
	CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.
	CC6.8* - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.
	CC7.4* - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
	CC7.5* - The entity identifies, develops, and implements activities to recover from identified security incidents.
Customers are responsible for notifying Appian of suspicious activities on the system and for taking appropriate actions for any suspicious activities reported to them by Appian.	CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
	CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
	CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

User Entity Control	Associated Criteria
	CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
	CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
	CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
	CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
	CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
	CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
	CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
	CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.
Customers are responsible for performing security testing against their sites as necessary.	CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
	CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

User Entity Control	Associated Criteria
	CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
	CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
	CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
	CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
	CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
	CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
	CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
	CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.
Each customer is responsible for the administration of external access to its Appian Cloud site.	CC5.2* - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

User Entity Control	Associated Criteria
	CC6.2* - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	CC6.3* - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Configuration and security of Appian applications and integrations built on Appian Cloud is the responsibility of the customer.	CC5.2* - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
	CC8.1* - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for validating their Appian application user accounts.	CC5.2* - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
	CC6.2* - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	CC6.3* - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Premier customers are responsible for creating and managing the encryption keys.	CC5.2* - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
	CC6.1* - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	CC6.6* - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

User Entity Control	Associated Criteria
	CC6.7* - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
Appian's customers are responsible for confidentiality and security measures over their data.	CC5.2* - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
	CC6.1* - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	CC6.2* - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	CC6.3* - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
	CC6.6* - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
	CC6.7* - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
	CC6.8* - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
Appian enables customers to integrate Appian Cloud with external systems through standard entry points. Customers are responsible for designing, configuring and implementing system integrations in a way that data is securely transferred across the interconnected systems.	CC5.2* - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
	CC6.1* - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

User Entity Control	Associated Criteria
	CC6.2* - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	CC6.3* - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
	CC6.6* - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
	CC6.7* - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
	CC6.8* - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
Customers are able to audit the Application Server logs as frequently as necessary and are responsible for notifying Appian of any suspicious activities which they consider may compromise the security of the system.	CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.
	CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
	CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
	CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
	CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

User Entity Control	Associated Criteria
	CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
	CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
	CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
	CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.
Each customer is responsible for implementing its own development methodologies for the applications built on Appian software. Customers should follow Appian Best Practices, located on Appian Forum.	CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
	CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
For customer applications, customers are responsible for managing their own non-production environments to test any customer software applications used on Appian Cloud. Responsibility for the change control of the software between the development, test, and production environments is the responsibility of the customer.	CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
	CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for the data classification of their own data.	CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	C1.1 - The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality.

User Entity Control	Associated Criteria
Appian Cloud data handling, and associated security parameters about the data, is each customer's responsibility.	C1.1* - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
Customers are responsible for retention and disposal policies and procedures for data within their Appian Cloud applications.	CC6.5* - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
	C1.1* - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
	C1.2* - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

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