APPIAN CORPORATION

Appian Cloud

SOC for Service Organizations Report for the period of July 1, 2017 to June 30, 2018

Grant Thornton

Report of Independent Service Auditors issued by Grant Thornton LLP

Contents

I. Report of Independent Service Auditors

To the Board of Directors and Stakeholders
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 the Appian Cloud (the "System") were effective throughout the period July 1, 2017 to June 30, 2018 (the "specified period"), to provide reasonable assurance that the criteria for the security, availability, and confidentiality principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* ("applicable trust services criteria") were met, if complementary subservice organizations and user entity controls assumed in the design of Appian Corporation's controls operated effectively throughout the period July 1, 2017 to June 30, 2018.

The Company uses a subservice organization, Amazon Web Services (AWS), for the hosting of its System's infrastructure. Management's assertion indicates that certain applicable trust services criteria specified by the Company in Section III, *Appian Corporation's Description of its System*, under the section *Subservice Organizations*, can be met 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 these subservice organizations, 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 applicable trust services criteria specified in Section III, *Appian Corporation's Description of its System*, under the section *User Entity Controls*, can be met 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 Corporation is responsible for the System and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the applicable trust service criteria were met. Appian Corporation has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Appian Corporation 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 applicable trust services criteria were met, if complementary subservice organizations and user entity controls assumed in the design of Appian Corporation's controls operated effectively throughout the period July 1, 2017 to June 30, 2018. 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;
- Assessing the risks that controls were not effective to meet the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the System were effective to meet 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 applicable trust services criteria were met. 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, 2017 to June 30, 2018, to provide reasonable assurance that the applicable trust services criteria were met, if complementary subservice organizations and user entity controls assumed in the design of Appian Corporation's controls operated effectively throughout the period July 1, 2017 to June 30, 2018, is fairly stated, in all material respects.

Grant Thornton LLP

Atlanta, Georgia
July 11, 2018

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, 2017 to June 30, 2018, to provide reasonable assurance that the criteria for the security, availability, confidentiality principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* ("applicable trust services criteria") were met. Our description of the boundaries of the System is presented in Section III, *Appian Corporation's Description of its System,* and identifies the aspects of the System covered by our assertion.

The Company uses a subservice organization, Amazon Web Services (AWS), for the hosting of its System's infrastructure. Certain applicable trust services criteria, specified in Section III, *Appian Corporation's Description of its System*, under the section *Subservice Organizations* can be met 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.

Certain applicable trust services criteria, specified in Section III, *Appian Corporation's Description of its System*, under the section *User Entity Controls* can be met 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.

We have performed an evaluation of the effectiveness of the controls within the System throughout the period July 1, 2017 to June 30, 2018, to provide reasonable assurance that the criteria for the security, availability, and confidentiality principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* were met. Our description of the boundaries of the System is presented in Section III, *Appian Corporation's Description of its System,* and identifies the aspects of the System covered by our assertion. Appian Corporation'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 also presented in Section III, *Appian Corporation's Description of its System.*

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 the applicable trust services criteria are met.

We assert that the controls within the System were effective throughout the period July 1, 2017 to June 30, 2018, to provide reasonable assurance that the applicable trust services criteria were met, if complementary subservice organizations and user entity controls assumed in the design of Appian Corporation's controls operated effectively throughout the period July 1, 2017 to June 30, 2018.

III. Appian Corporation's Description 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") and only includes those control activities and related criteria surrounding those operations for the period of July 1, 2017 through June 30, 2018 (the "specified period") for the Security, Availability, and Confidentiality principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Trust Services Principles and Criteria*) ("applicable 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

As the market leader in modern Business Process Management (BPM) and Case Management software, Appian delivers an enterprise application platform that unites users with their data, processes, and collaborations – in one environment, on any mobile device, through a simple social interface.

Appian is committed to delivering a quality customer experience to its clients – through innovative technology and outstanding service. With more than 3.5 million users around the globe, Appian has a community of customers and partners across multiple industries and geographies. With a management team of industry veterans and a comprehensive implementation methodology, Appian helps to ensure the success of its customers' BPM initiatives.

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:

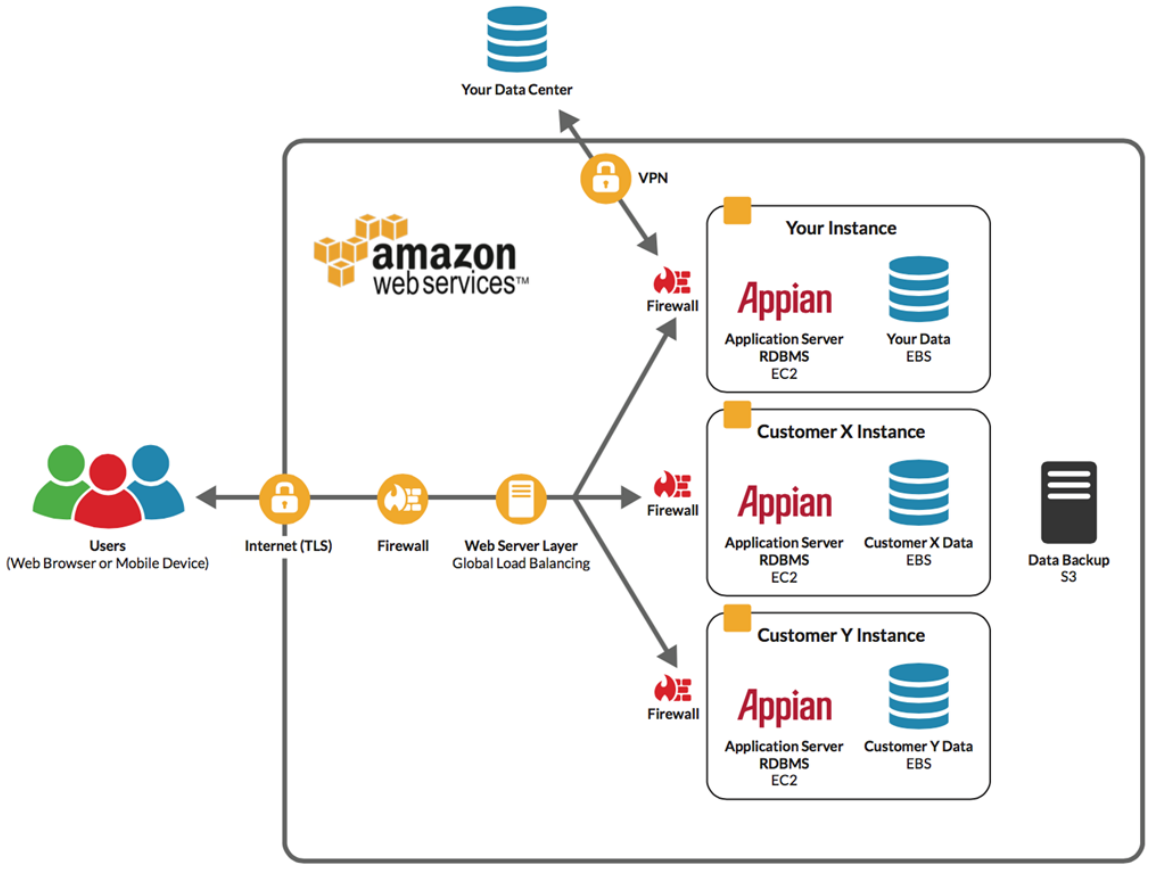
- Application Server,
- Appian Engine,
- Database,
- Operating System, and
- AWS EC2[2] Instance.

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,
- 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.

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

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. 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.

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), Availability (A), and Confidentiality (C) Trust Principles		
Non-Applicable Trust Services Criteria		**Appian Corporation's Rationale**
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel.	Appian's hosting provider, Amazon Web Services (AWS), is responsible for physical security controls.
C1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes in accordance with confidentiality commitments and requirements.	Customers should have their own development and test environments to test any customer software applications used on Appian Cloud. Responsibility for change control of the software between the development, test, and production environments is the responsibility of the customer.

Subservice Organizations

The Company utilizes a subservice organization to perform certain functions to improve operating and administrative effectiveness. The accompanying 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 service organization described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at this subservice organization. The most significant subservicing organization used by the Company is noted below.

Subservice Organization	Services Provided	Associated Criteria
Amazon Web Services (AWS)	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 Activity is critical to achieving the applicable trust services criteria: • Control activities, including environmental control activities, around the backup processes at the Data Centers hosting the in-scope applications to support the disaster recovery processes. 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.	CC5.5 - Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. A1.2* - Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.

Subservice Organization	Services Provided	Associated Criteria
	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 Type II reports, etc. Corrective actions are taken, if necessary, based on the results of these reviews.	

* 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

The processes of the Company were designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at user organizations is necessary to achieve the applicable trust services criteria included in this report.

This section highlights those internal control responsibilities that the Company believes should be present for each user organization and has considered in developing its control policies and procedures described in this report. In order for users to rely on the control structure's policies and procedures reported on herein, each user must evaluate its own internal control structure to determine if the following procedures are in place. Furthermore, the following list of control policies and procedures is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user. Accordingly, this list does not allege to be, and is not, a complete listing of the control policies and procedures that provide a basis for management's assertions related to the applicable trust services criteria.

User Entity Control	Associated Criteria
Customers are responsible for requesting the description of Appian Cloud.	CC2.1* - Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their roles in the system and the results of system operation.

User Entity Control	Associated Criteria
Customers are responsible for providing training to users of the application(s) built on Appian Cloud.	CC2.2* - The entity's security, availability, and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.
	CC2.3* - The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.
	CC2.5* - Internal and external users have been provided with information on how to report security, availability, and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.
Customers are responsible for reviewing and approving changes that may affect system security, availability, and/or confidentiality.	CC2.2* - The entity's security, availability, and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.
	CC2.3* - The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.
	CC2.5* - Internal and external users have been provided with information on how to report security, availability, and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.
	CC2.6* - System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security, availability, and confidentiality are communicated to those users in a timely manner.
Customers are responsible for controlling who has access to their data and for alerting Appian of any unauthorized access and/or issues/breaches.	CC2.2* - The entity's security, availability, and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.
	CC2.3* - The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.

User Entity Control	Associated Criteria
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.	CC3.1* - The entity (1) identifies potential threats that could impair system security, availability, and confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.
	CC6.2* - Security, availability, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.
	CC7.3* - Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

User Entity Control	Associated Criteria
Customers are responsible for performing security testing against their sites as necessary.	CC3.1* - The entity (1) identifies potential threats that could impair system security, availability, and confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.
	CC6.1* - Vulnerabilities of system components to security, availability, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly-identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
Each customer is responsible for the administration of external access to its Appian Cloud site.	CC5.1* - Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

User Entity Control	Associated Criteria
	CC5.2* - New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and are granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	CC5.3* - Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
	CC5.4* - Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
	CC5.6* - Logical access security measures have been implemented to protect against security, availability, and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.
	CC5.7* - The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security, availability, and confidentiality.
	CC5.8* - Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
	C1.3* - Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.

User Entity Control	Associated Criteria
Configuration and security of Appian applications and integrations built on Appian Cloud is the responsibility of the customer.	CC5.1* - Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
	CC5.2* - New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and are granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	CC5.4* - Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
	CC5.6* - Logical access security measures have been implemented to protect against security, availability, and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.
Customers are responsible for validating their Appian application user accounts.	CC5.4* - Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
	CC5.6* - Logical access security measures have been implemented to protect against security, availability, and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.

User Entity Control	Associated Criteria
Appian's customers are responsible for confidentiality and security measures over their data.	CC5.4* - Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
	C1.2* - Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.
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.	CC5.6* - Logical access security measures have been implemented to protect against security, availability, and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.
	CC5.7* - The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security, availability, and confidentiality.
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.	CC6.2* - Security, availability, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.
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.	CC7.1* - The entity's commitments and system requirements, as they relate to security, availability, and confidentiality, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.

User Entity Control	Associated Criteria
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.	C1.1* - Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.
Customers are responsible for the data classification of their own data.	C1.2* - Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.
	C1.6* - Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.
Appian Cloud data handling, and associated security parameters about the data, is each customer's responsibility.	C1.2* - Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.
	C1.7* - The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.
Customers are responsible for retention and disposal policies and procedures for data within their Appian Cloud applications.	C1.7* - The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.
	C1.8* - The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.

* This is a complementary control and is required to achieve design and operating effectiveness for this particular criterion.