APPIAN CORPORATION

Appian Cloud

SOC for Service Organizations Report for the period of July 1, 2016 to June 30, 2017

Grant Thornton

Report of Independent Service Auditors issued by Grant Thornton LLP

Contents

I. Report of Independent Service Auditors 1

II. Appian Corporation's Assertion 3

III. Appian Corporation's Description of its System and Controls 4

A. Scope and Purpose of the Report 4

B. Overview of Services Provided 4

C. Non-Applicable Trust Services Criteria 7

D. Subservice Organizations 8

E. User Control Considerations 9

I. Report of Independent Service Auditors

To the Board of Directors and Stakeholders:
Appian Corporation

We have examined Appian Corporation's (the "Company" or "Appian") accompanying assertion in *Section II, Appian Corporation's Assertion*, that, during the period July 1, 2016 to June 30, 2017 (the "Specified Period"), Appian Corporation maintained, in all material respects, effective controls over Appian Cloud (the "System") to provide reasonable assurance that the System was protected against unauthorized access (both physical and logical), that the system was available for operation and use as committed to or agreed upon, and that information designated as confidential was protected as committed to or agreed upon, based on the American Institute of Certified Public Accountant's (AICPA's) Trust Services Principles criteria for the Security, Availability, and Confidentiality Trust Principles set forth in TSP Section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) ("AICPA Applicable 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 also indicates that certain AICPA Applicable Trust Services Criteria specified by management in *Section III, Appian Corporation's Description of its System and Controls*, under the *Subservice Organizations Section*, can be achieved only if the 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 organization controls.

Management's assertion indicates that certain AICPA Applicable Trust Services Criteria specified in *Section III, Appian Corporation's Description of its System and Controls*, under the *User Control Considerations Section*, 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.

In Section II of the report, the Company has provided its assertion, which is based on the criteria identified in management's assertion about the suitability of design and operating effectiveness of controls to meet the Applicable Trust Services Criteria. The Company's management is responsible for preparing its assertion, including the completeness, accuracy, and method of presentation of Appian Corporation's Description of its System and Controls; selecting the Applicable Trust Principles; identifying the risks that threaten the Applicable Trust Services Criteria from being met; selecting the criteria stated in the assertion; and designing, implementing, and documenting controls that are suitably designed and operating effectively to meet the Applicable Trust Services Criteria.

Our responsibility is to express an opinion based on our examination of the description criteria in management's assertion, on the suitability of the design and operating effectiveness of the controls to meet the Applicable Trust Services Criteria, based on our examination. Management's description of the aspects of the System covered by its assertion is attached in *Section III, Appian Corporation's Description of its System and Controls*. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of the Company's relevant controls over the System that meet the AICPA's Trust Services Principles criteria for Security, Availability, and Confidentiality; (2) testing and evaluating the suitability of the design and operating effectiveness of the controls, which together with the complementary user entity controls and the complementary subservice organization (Amazon Web Services) controls referred to above, if operating effectively, were those necessary to provide reasonable assurance that the Applicable Trust Services Criteria were met; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of their nature and inherent limitations, controls at a service organization may not always protect information against unauthorized access or use, make the system available for operation and use as committed to or agreed upon, and protect information designated as confidential as committed to or agreed upon.

For example, fraud or unauthorized access to systems and information, or unauthorized use or disclosure of information by persons authorized to access it, may not be prevented or detected or controls may fail to comply with internal and external policies or requirements. Also, the projection of any conclusions, based on our findings, to future periods is subject to the risk that any changes or future events may alter the validity of such conclusions.

In our opinion, the Company's assertion for the Specified Period referred to above is fairly stated, in all material respects, based on the AICPA's Applicable Trust Services Criteria.

Grant Thornton LLP

Atlanta, Georgia
July 10, 2017

II. Appian Corporation's Assertion

We, the management of Appian Corporation (the "Company" or "Appian") assert that, during the period July 1, 2016 through June 30, 2017 (the "Specified Period"), the Company maintained, in all material respects, effective controls over Appian Cloud (the "System") to provide reasonable assurance that the System was protected against unauthorized access (both physical and logical), that the system was available for operation and use as committed to or agreed upon, and that information designated as confidential was protected as committed to or agreed upon, based on the American Institute of Certified Public Accountant's (AICPA) Applicable Trust Services Criteria set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("AICPA Applicable 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 also indicates that certain AICPA Applicable Trust Services Criteria specified by management in *Section III, Appian Corporation's Description of its System and Controls*, under the *Subservice Organizations Section*, can be achieved only if the 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 organization controls.

Certain AICPA Applicable Trust Services Criteria, specified *in Section III, Appian Corporation's Description of its System and Controls*, under the *User Control Considerations Section* 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 description in Section III of this report includes only the controls of the Company and excludes the controls performed by User Entities.

Our description of this System in Section III of this report identifies the aspects of the System covered by our assertion.

III. Appian Corporation's Description of its System and Controls

A. Scope and Purpose of the Report

This report describes the control structure of Appian Corporation's (the "Company" or "Appian") Appian Cloud and only includes those control activities and the related criteria surrounding those operations for the period of July 1, 2016 to June 30, 2017 (the "Specified Period"), for the Security, Availability, and Confidentiality Trust Services Principles. This report does not include control activities surrounding any other services or locations that are specifically excluded from the report but are performed by the Company.

The description is intended to provide customers and user entities of the Company's System, those prospective user entities, independent auditors, practitioners providing services to such user entities, and other specified parties with information about the control features of the Company's System to enable customers of the Company to plan their audits. The description is intended to provide users with information about the System, particularly system controls intended to meet the criteria for the Security, Availability, and Confidentiality Trust Services Principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (American Institute of Certified Public Accountants, *Trust Services Principles and Criteria*) (the "Applicable Trust Services Criteria"). It was prepared taking into consideration the attestation standards established by the American Institute of Certified Public Accountants (the "AICPA"). As this description is intended to focus on features that may be relevant to the internal control of Appian's customers and other specified parties, it does not encompass all aspects of the services provided or procedures followed by Appian.

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 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.

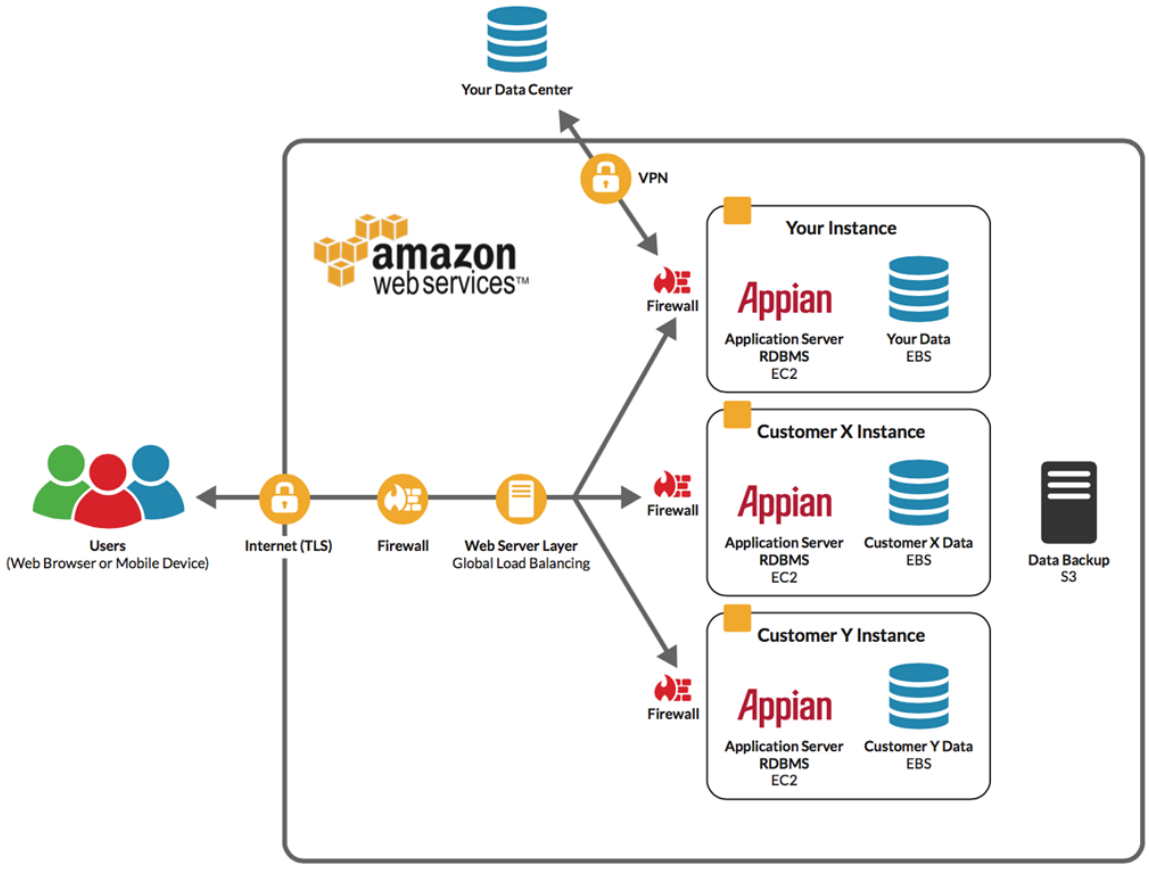
The following exist in the AWS environment to support Appian Cloud sites:

- 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 multifactor 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. 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.

D. 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: • Controls, including environmental controls, 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, management evaluates the performance of the third-party organization to help ensure its compliance with commitments and agreed-upon service level agreements.	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.

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

E. User Control Considerations

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 AICPA's Applicable Trust Services Criteria included within this report.

This Section highlights those internal control responsibilities which the Company believes should be present for each user organization and has considered in developing its control policies and procedures described within 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 AICPA's 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.
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.

User Entity Control	Associated Criteria
	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.
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.

User Entity Control	Associated Criteria
	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.
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.
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.

User Entity Control	Associated Criteria
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.

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