



BRAZE, INC.

SOC 2 REPORT

FOR

BRAZE SERVICES

**A TYPE 2 INDEPENDENT SERVICE AUDITOR'S
REPORT ON CONTROLS RELEVANT TO SECURITY**

JANUARY 1, 2018, TO JUNE 30, 2018

Attestation and Compliance Services



Proprietary & Confidential

Reproduction or distribution in whole or in part without prior written consent is strictly prohibited.

This report is intended solely for use by the management of Braze, Inc., user entities of Braze, Inc.'s services, and other parties who have sufficient knowledge and understanding of Braze, Inc.'s services covered by this report (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2	MANAGEMENT'S ASSERTION	4
SECTION 3	DESCRIPTION OF THE SYSTEM	7
SECTION 4	TESTING MATRICES	19

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Braze, Inc.:

Scope

We have examined the attached description of Braze, Inc.'s ("Braze" or the "service organization") Braze Services system for the period January 1, 2018, to June 30, 2018, (the "description") performed at the New York, New York, facility based on the criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* ("description criteria") and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security principle set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)* ("applicable trust services criteria"), throughout the period January 1, 2018, to June 30, 2018.

As indicated in the description, Braze uses various subservice organizations for Infrastructure as a Service and Database as a Service. The description indicates that certain applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at subservice organizations are suitably designed and operating effectively. The description presents Braze's system; its controls relevant to the applicable trust services criteria; and the types of controls that Braze expects to be implemented, suitably designed, and operating effectively at subservice organizations to meet certain applicable trust services criteria. The description does not include any of the controls expected to be implemented at subservice organizations. Our examination did not extend to the services provided by subservice organizations, and we have not evaluated whether the controls management expects to be implemented at subservice organizations have been implemented or whether such controls were suitably designed and operating effectively throughout the period January 1, 2018, to June 30, 2018.

Service organization's responsibilities

Braze has provided the attached assertion, in Section 2, about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Braze is responsible for preparing the description of the service organization's system and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description of the service organization's system; selecting the trust services principle(s) addressed by the engagement and stating the applicable trust services criteria and related controls in the description of the service organization's system; identifying the risks that would prevent the applicable trust services criteria from being met; identifying any applicable trust services criteria related to the principle(s) being reported on that have been omitted from the description and explaining the reason for the omission; and designing, implementing, and documenting controls to meet the applicable trust services criteria.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period January 1, 2018, to June 30, 2018.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and that the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period January 1, 2018, to June 30, 2018. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust

services criteria were met. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the description criteria identified in Braze's assertion and the applicable trust services criteria

- a. the description fairly presents the system that was designed and implemented throughout the period January 1, 2018, to June 30, 2018;
- b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period January 1, 2018, to June 30, 2018, and subservice organizations applied the types of controls expected to be implemented at subservice organizations throughout the period January 1, 2018, to June 30, 2018; and
- c. the controls that were tested, which were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period January 1, 2018, to June 30, 2018 if the controls expected to be implemented at subservice organizations were also operating effectively throughout the period January 1, 2018, to June 30, 2018.

Description of test of controls

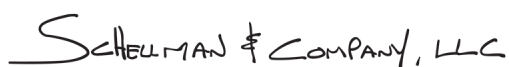
The specific controls we tested, and the nature, timing, and results of our tests are presented in section 4 of our report titled "Testing Matrices."

Restricted use

This report, including the description of tests of controls and results thereof in section 4 are intended solely for the information and use of Braze; user entities of the Braze Services system during some or all of the period January 1, 2018, to June 30, 2018; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, subservice organizations, or other parties;
- Internal control and its limitations;
- The nature of user entity controls responsibilities and their role in the user entities internal control as it relates to, and how they interact with, related controls at the service organization;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

SCHHELLMAN & COMPANY, LLC

Tampa, Florida
August 3, 2018

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the attached description of the Braze Services system for the period January 1, 2018, to June 30, 2018, (the "description") based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (the "description criteria"). The description is intended to provide users with information about the Braze Services system, particularly system controls intended to meet the criteria for the security principle set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)* ("applicable trust services criteria"). We confirm, to the best of our knowledge and belief, that

- a. the description fairly presents the Braze Services system throughout the period January 1, 2018, to June 30, 2018, based on the following description criteria:
 - i. The description contains the following information:
 - 1.) The types of services provided;
 - 2.) The components of the system used to provide the services, which are the following:
 - a.) *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks)
 - b.) *Software*. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities)
 - c.) *People*. The personnel involved in the governance, operation and use of a system (developers, operators, entity users, vendor personnel, and managers)
 - d.) *Procedures*. The automated and manual procedures
 - e.) *Data*. Transaction streams, files, databases, tables, and output used or processed by a system;
 - 3.) The boundaries or aspects of the system covered by the description;
 - 4.) For information provided to, or received from, subservice organizations and other parties
 - a.) How such information is provided or received and the role of the subservice organizations and other parties
 - b.) The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls;
 - 5.) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:
 - a.) Complementary user entity controls contemplated in the design of the service organization's system
 - b.) When the inclusive method is used to present a subservice organization, controls at the subservice organization;
 - 6.) If the service organization presents the subservice organization using the carve-out method
 - a.) The nature of the services provided by the subservice organization
 - b.) Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria;
 - 7.) Any applicable trust services criteria that are not addressed by a control and the reasons; and

- 8.) In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the description.
- ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual report user may consider important to its own particular needs.
- b. the controls stated in the description were suitably designed throughout the specified period to meet the applicable trust services criteria.
 - c. the controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Braze (formerly Appboy) is a customer relationship management (CRM) and marketing automation platform designed to help brands build better relationships with their customers. Founded in 2011, Braze has offices in New York, San Francisco, Singapore, and London, and services over 500 global clients spanning 35 countries.

Description of Services Provided

Braze is a platform that enables its clients to build and deliver personalized messaging campaigns with real-time reporting and optimization that is scalable. A web-based dashboard allows Braze clients to build relationships with their customers through relevant, cross-channel campaigns based on customer behavior.

With the Braze dashboard, teams can achieve:

- Cross-channel campaigns: Compose, preview, test, and send messaging campaigns across supported channels (iOS/Android Push, In-App Messaging, News Feed, E mail, and HTTP webhooks).
- Personalization: Quickly identify customer segments based on behaviors and other characteristics aggregated through a single view of each individual customer, allowing for relevant, highly-personalized messaging.
- Lifecycle Engagement Orchestration: Use the Braze visual drag-and-drop experimentation tool, Canvas, to orchestrate campaigns across multiple channels, including push, in-app messaging, and e-mail.
- Optimization and artificial intelligence (AI): Continually test, iterate, and optimize, taking learnings from successes to build future campaigns.
- Data management and agility: Extract value from large amounts of data quickly and translate that information into action with our high-volume data export tool, Currents. Relevant data is centralized in Braze through a variety of methods:
 - Tagging directly to various Braze Services software development kits (SDKs);
 - Sending to the Braze REST application programming interface (API); and
 - Uploading manually in the Braze dashboard via comma separated values (CSV) file.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

Braze utilizes AWS and Rackspace for Infrastructure as a Service (IaaS) and Database as a Service (DBaaS), respectively. AWS and Rackspace are responsible for providing physical safeguarding of information technology (IT) infrastructure. AWS and Rackspace are also responsible for providing environmental safeguards (e.g. power supply, temperature control, fire suppression, etc.) against certain environmental threats. Additional AWS and Rackspace responsibilities include managing logical access to the underlying network, virtualization management, and storage devices for its IaaS data hosting services where Braze systems reside. In providing DBaaS services, Rackspace is responsible for providing single-tenant, container-based environment for Braze's databases. Braze is responsible for the platform and the customer is responsible for configuring the software as they see fit

(including access/password/session controls, what data they choose to store, workflow, etc.). The production infrastructure resides within AWS US and Frankfurt data centers and the Rackspace data center in Ashburn, VA.

The in-scope infrastructure consists of multiple systems as shown in the table below:

Primary Infrastructure			
Production System	Business Function Description	Platform	Physical Location
AWS Security Groups	This is the “firewall” feature provided by AWS EC2	AWS proprietary	AWS
Servers	Virtual machines supporting the Braze Service residing in the AWS EC2 instance	Linux	
Database	Braze application customer data storage	MongoDB	Rackspace, AWS
Braze Application	Braze Services	Linux	AWS
Virtual Private Network (VPN)	Provides access control, endpoint security, and authentication and authorization services to the production environments	Open VPN	AWS

People

The personnel involved in the operation and use of a system are as follows:

- Senior Management – responsible for setting company direction and strategy
- Chief Technology Officer (CTO) – responsible for overall technology and engineering posture of Braze, as well as member of Senior Management Team.
- Director of DevOps and Security – responsible for leading DevOps, infrastructure, operations, and security at Braze.
- DevOps – responsible for continuous monitoring of applications and infrastructure; automation of tasks, processes, and workflows; and implementation of infrastructure as code.
- Information Security Manager – responsible for implementing information security program at Braze.
- IT – responsible for the daily operations for the Braze and working with customers to perform environment changes and application upgrades.
- Human Resources (HR) – responsible for creating and implementing human resources policies at Braze.
- Customer Success – responsible for onboarding customers, as well as providing technical and strategic support.

Procedures

HR Hiring and Termination

Organizational charts are in place to communicate key areas of authority, responsibility, and lines of reporting to personnel. Charts are communicated to employees through direct integration with the HR site, and are updated in real-time. Across the organization, documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs. HR maintains new employee hiring procedures to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description. Background checks are performed for employees working with customer data as a component of the hiring process.

New hire employees are required to complete an acknowledgement form documenting their receipt and understanding of the employment policies which communicates workplace conduct standards, acceptable user, and information security policies. New hire employees are also required to sign a nondisclosure agreement when their employment begins. Additionally, employees are required to complete security awareness training upon hire and on an annual basis to understand their obligations and responsibilities to comply with security policies. Termination procedures are initiated by the HR department and disseminated to the appropriate Braze teams.

Training courses are available on an online training portal to new and existing employees to help maintain and advance the skill level of personnel. Documented policies and procedures are in place to govern the provision of training and other resources to support system security policies.

Access Authentication and Authorization

Braze production systems are hosted within AWS and Rackspace environments. Authentication to the AWS and Rackspace portals requires an authorized username and password. Only authorized Braze personnel have the ability to log into these portals to perform privileged functions.

In order to connect directly to a Braze production server, a user must first connect to the VPN that requires two-factor authentication. Users must first authenticate into the VPN via their Active Directory credentials, and once authenticated, the system automatically performs a system check to ensure that a required user certificate has been installed for the user's workstation, providing a second authentication factor before the VPN connection is created. Once connected to the VPN, a user is then allowed to login to a server. Users are required to authenticate with a valid user account and secure shell (SSH) private key pair before being granted access to the Linux server operating system. Additionally, users must have a profile created for them on the server they are connecting to, as well as the CHEF management server that governs access within the environment. For European databases, database users are required to authenticate via authorized shared user account and password maintained within the CHEF server management system before being granted access to the database. US based databases are managed by Rackspace and Braze employees do not have access to log into the databases directly. Administrative access to the AWS and Rackspace production environment is restricted to authorized personnel. Additionally, administrative access on the servers and databases is also restricted to authorized IT personnel.

When attempting to authenticate to the Braze application, users are prompted to enter a username and password. Customer accounts are initially set up by the Braze administrators via the Braze application's Success Manager administrator portal. Once the customer account is created, the customer has the ability to add, modify or remove user accounts. Only authorized Braze personnel have the ability to grant access to the administrative portal to other Braze employees.

Access Requests and Access Revocation

Documented information security policies and procedures are in place to guide personnel in information security practices including access administration. When a new employee joins the company, and if an existing employee requires additional/modified access, IT personnel utilize a ticketing system to request and approve required system access. In order for access to be granted, an approval must be obtained by authorized management, consisting of the director of DevOps and Security or the CTO. Access is then assigned accordingly by IT personnel.

On a quarterly basis, a review of user access rights to the production environment is performed. Access rights that are deemed unnecessary or not commensurate with the user's job responsibilities are removed or altered as necessary by IT management. Termination procedures are initiated by HR. HR notifies IT personnel of employee terminations via the Bamboo HRIS system, and IT personnel revoke terminated employees' access, as applicable, upon receipt of the notification.

Change Management

Documented change management policies and procedures are in place to guide personnel in performing change management procedures. On a monthly basis, change management meetings are held to discuss ongoing and upcoming change releases.

An overall project management tool is utilized to track the lifecycle of application changes whether they be features or bug fixes. A separate ticketing system is utilized to track the actual development activities, testing, and approvals. A change ticket is created detailing the change (change description), involved parties, testing details, approval, and backout plans. Change tickets can be opened by a software engineer 2 and above. Development and testing efforts are performed in development and test environments that are logically separate from the production environment. A version control system is utilized to control access to source code and to track change activities.

Day to day development activities are performed in segmented development branches, each belonging to a specific development team member. Quality assurance (QA) testing and approvals are required to be performed prior to merging code from these segmented branches to the master code branch. When a change is ready to be merged with the master code branch, engineers create pull requests, which systemically pulls code into the master branch. Only authorized personnel have the ability to pull the code over to the master branch and personnel cannot commit directly to the master branch. Continuous Integration (CI) tests are configured to automatically run upon merging code into the master branch. If the CI test fails, an e-mail is sent to the members involved in the change at which point, required updates and fixes are made. A CI test is then rerun until successful completion.

An automated deployment tool is utilized to manage the deployment process. The ability to deploy a change from the master code branch to the production environment is restricted to user accounts accessible by authorized IT personnel, and the system is configured to require that changes must be approved by a user separate from the developer in order to be migrated into production.

In the event that a change must be made quickly, the segregation between approver and deployer can be overridden; this is considered an emergency change. The deployment tool is configured to log when this override function is used such that instances where the same user approved a change also implements the change, can be identified in audit logs. The instance of override activity must be reviewed within 24 hours by another development staff member after the completion of the emergency change, in accordance with the change management policies and procedures. The review and approval of the change is documented. Only authorized personnel have the ability to override the segregation of duties function enforced by the deployment tool.

In addition to application code changes, Braze patches its servers on a regular basis and Braze's configuration management system regularly applies patches via Linux repositories. Patches are tested prior to being implemented into production.

Data Backup

An automated backup system is utilized to perform scheduled system backups of production application and data files on a daily basis. The automated backup system is configured to send e-mail alert notifications to IT personnel regarding backup failures. Backups are managed by AWS and Rackspace.

Network Security

Documented network security policies and procedures are in place to guide personnel in network security practices. In the AWS environment, a firewall utility is in place to filter unauthorized inbound network traffic from the Internet and are designed to deny any network connection that is not explicitly authorized by a security group rule. Braze manages these security groups. In the Rackspace environment, network security is managed fully by Rackspace. Externally routable Internet Protocol (IP) addresses are not utilized for the hosted application and database servers. Administrator access within the firewall utility is restricted to user accounts accessible by authorized IT personnel.

A third-party specialist performs an external penetration assessment on an annual basis. Operations and IT management review the results of the penetration assessments and create remediation and mitigation plans where required.

To protect data while in transit, web servers utilize transport layer security (TLS) encryption for web communication sessions. Additionally, an encrypted VPN is utilized to protect sessions between personnel and the production environment.

System Monitoring and Incident Response

Braze employs an information security program consisting of a set of policies and standards that include, but are not limited to, computer usage guidelines, acceptable use of IT assets, incident handling, and security administration procedures. Additionally, documented escalation procedures for reporting security incidents are communicated to internal users via the customer contracts site to provide guidance in identifying and reporting failures, incidents, concerns, and other complaints. External users can contact Braze's incident response personnel via the customer support tab, available on each customers' dashboard, in order to report system failures, incidents, concerns, and other complaints. The customer facing website provides guidance to external users should they need to contact Braze's incident response personnel.

Management meetings are held on at least a monthly basis to discuss incidents and corrective measures to help ensure that incidents are resolved. IT operations personnel utilize a ticketing system to document security violations, responses, and resolution. Incidents requiring a change to the system follow the standard change control process.

Data

The customer data stored within the Braze Services is owned and managed by the customer. The customer is wholly responsible for the data entry and management processes. Customer data that resides on Braze systems is treated as Confidential.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Customer campaign design information	Standard and customized report writing tools are available	Confidential
Customer campaign results	Standard and customized report writing tools are available	Confidential
Data regarding campaign target audiences and subsets	Standard and customized report writing tools are available	Confidential

Significant Changes During the Review Period

No relevant changes to the Braze Services system occurred during the review period.

Subservice Organizations

The IaaS services provided by AWS and the DBaaS services provided by Rackspace were not included within the scope of this examination. Therefore, the description does not address the (a)(i)(4) and (a)(i)(5)(b) criteria in Section 2.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS and Rackspace, alone or in combination with controls at Braze, and the types of controls expected to be implemented at AWS and Rackspace to meet those criteria.

Control Activity Expected to be Implemented by AWS & Rackspace	Applicable Trust Services Criteria
AWS and Rackspace are responsible for ensuring logical access to the underlying network, virtualization management, and storage devices for the IaaS and DBaaS services where Braze systems reside.	CC5.1 – CC5.4 CC5.6

Control Activity Expected to be Implemented by AWS & Rackspace	Applicable Trust Services Criteria
AWS and Rackspace are responsible for ensuring controls for restricting physical access to data center facilities, backup media, and other system components including network devices, virtualization, and storage infrastructure.	CC5.5

CONTROL ENVIRONMENT

The control environment at Braze is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and operations management.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of the entity's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct and by example. Specific control activities that Braze has implemented in this area include the following:

- Organizational policy statements and codes of conduct are documented and communicate entity values and behavioral standards to personnel.
- Employees are required to sign acknowledgement of receipt of the basic employment policies describing workplace conduct agreeing to complete a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- Employees are required to complete security awareness trainings upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.
- Background checks are performed for employees as a component of the hiring process.

Board of Directors and Audit Committee Oversight

Braze's control consciousness is influenced significantly by the entity's executive management and board of directors. Attributes include the board of directors' independence from management, the experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management, and its interaction with external auditors. The Braze board of directors oversees the company's operations. The board of directors meets at planned intervals each quarter.

Organizational Structure and Assignment of Authority and Responsibility

Braze's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Braze's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and designated

lines of reporting. Braze has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Braze's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at helping to ensure that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational reporting lines are in place to communicate key areas of authority, responsibility, and designated lines of reporting to personnel. These charts are shared with employees on the company's intranet and updated as needed with every new hire or termination.

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Specific control activities that Braze has implemented in this area include the following:

- Management considers the competence levels for particular jobs and translates the required skills and knowledge levels into written position requirements.
- Job candidates are required to demonstrate prerequisite skills and knowledge prior to being hired.
- Internal training on security and job-related skills are performed as a component of the new hire process.

Accountability

Braze's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel. The management team provides overall direction, policies, and goals for the organization. Specific control activities that Braze has implemented in this area are described below.

- Management monitors regulatory and industry changes affecting services provided.
- Board meetings are held on a quarterly basis to discuss strategy.
- Operational management meetings are held monthly to discuss operational performance and issues.

Braze's HR policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that the service organization has implemented in this area are described below:

- Established pre-hire screening procedures are performed for personnel.
- A termination checklist is completed to help ensure that employee access is revoked from systems as a component of the termination process.

RISK ASSESSMENT

An analysis of the Braze information networks and systems is conducted on an annual basis to document the threats and vulnerabilities to stored and transmitted information. The analysis examines the types of threats (i.e. internal/external, natural/manmade, electronic/non-electronic) that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities which potentially expose the information

resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination, and protection. From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity, and availability of the information, is assigned. These risks are documented within the tracking tool in order to be monitored until remediated.

Risk Identification

Braze has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user entities. Key members of the executive management, IT, and operational teams meet on a quarterly basis to identify and review risks to the system. These risks are documented in a tracking spreadsheet managed by the Information Security Manager.

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Risk Analysis

Risk analysis is an essential process to the entity's success. It includes identification of key business processes where potential exposures of some consequence exist, as well as significant changes to those processes. Management has implemented a process whereby the likelihood and impact of various risks to the in-scope services have been assessed. Management broadly defines risk levels to the identified risks, according to the following three categories: Low Risk, Medium Risk, or High Risk. Where possible, a mitigation plan is created and implemented to reduce the level of risk. If the level of risk cannot be reduced, then the controls continue to be a part of continuous review and consideration. Management has identified control activities designed to mitigate the risks associated with the applicable criteria within scope. These control activities are documented below, in Section 4. Additionally, management reviews the assessed risk levels on an annual basis and documents the risk assessment in the annual risk program.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security principle.

Selection and Development of Control Activities

The applicable trust criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Braze's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security are applicable to the Braze Services system. Therefore, the description does not address the (a)(i)(7) criteria in Section 2.

INFORMATION AND COMMUNICATION SYSTEMS

Pertinent information must be identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial, and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities, and conditions necessary to inform business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. Personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers and suppliers.

Internal Communication

Communication takes such forms as policy, manuals, and memoranda. Communications also can be made electronically, verbally, and through the actions of management. Employees are encouraged to communicate to their lead/mentor, manager, or senior management. Braze has an employee handbook, code of conduct, and security policies documented to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of e-mail to communicate time sensitive information and processes for security purposes that notify key personnel in the event of problems.

External Communications

Braze has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in processing their transactions and communication of significant events. These methods include informal discussions with representatives from customers and the use of e-mail messages and customer contacts to communicate time-sensitive information. Braze also provides a summary of security policies in place at Braze to customers. Additionally, a 'Security, Privacy, and Architecture Information Security Datasheet' document is maintained and shared. This document provides Braze's customers with a detailed listing of the controls that are implemented and maintained to protect the security of the Braze Services as well as a clear communication of the customer's responsibilities in achieving security of the system.

If incidents are communicated, personnel follow documented incident response plan. Incidents are documented within the ticketing system and tracked by management until resolved.

MONITORING

Braze's management performs monitoring activities in order to continuously assess the quality of internal control over time. Monitoring activities are used to initiate corrective action through department meetings, client conference calls, and informal notifications. Management performs monitoring activities on a continuous basis and necessary corrective actions are taken as required to correct deviations from company policy and procedures.

Monitoring can be done in two ways: through ongoing activities or separate evaluations. The greater the degree and effectiveness of ongoing monitoring, the less the need is for separate evaluations. Management determines the need for separate evaluations by consideration given to the following: the nature and degree of changes occurring and their associated risks, the competence and experience of the people implementing the controls, as well as the results of the ongoing monitoring. Management has implemented a combination of ongoing monitoring and separate evaluations, as deemed necessary, to help ensure that the internal control system maintains its effectiveness over time.

Ongoing Monitoring

Examples of Braze's ongoing monitoring activities include the following:

- In carrying out its regular management activities, operating management obtains evidence that the system of internal control continues to function.
- Communications from external parties and customers corroborate internally generated information or indicate problems.
- Organizational structure and supervisory activities provide oversight of control functions and identification of deficiencies.
- Amazon CloudWatch cloud monitoring service is utilized to monitor the performance and availability of production systems and associated devices.
- Amazon CloudTrail is used to log AWS API and web console activity including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.
- Rackspace Monitoring is used to monitoring the performance and availability of production databases.

Separate Evaluations

Evaluation of an entire internal control system may be prompted by a number of reasons: major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods of processing financial information. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk will tend to be evaluated more often.

Often, evaluations take the form of self-assessments, where persons responsible for a particular unit or function will determine the effectiveness of controls for their activities. These assessments are considered by management, along with any other internal control evaluations. The findings of these efforts are utilized to help ensure follow-up actions are taken and subsequent evaluations are modified as necessary.

Subservice Organization Monitoring

IaaS and DBaaS services provided by AWS and Rackspace are monitored on a regular basis as part of the day-to-day business operations. On a more formal basis, Braze performs an annual review of the AWS and Rackspace third party examination reports. If any findings or issues require follow up, the security group will investigate and follow up with the service providers as necessary.

Evaluating and Communicating Deficiencies

Deficiencies in management's internal control system surface from many sources, including the company's ongoing monitoring procedures, separate evaluations of the internal control system and external parties. Management has developed protocols to help ensure findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and makes the decision to address deficiencies based on whether the incident was isolated or requires a change in the company's procedures or personnel.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Complementary user entity controls are not required, or significant, to achieve the applicable trust services criteria. Therefore, the description does not address the (a)(i)(5)(a) criteria in Section 2.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Braze Services system provided by Braze. The scope of the testing was restricted to the Braze Services system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period January 1, 2018, to June 30, 2018.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g. approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by subservice organizations, in order to complement the control activities and achieve the applicable trust services criteria, are presented in the “Subservice Organizations” section within Section 3.

SECURITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.0: Common Criteria Related to Organization and Management			
CC1.1: The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security.			
CC1.1.1	Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. These charts are communicated to employees and updated in real time.	Inquired of the CTO regarding organizational management to determine that organizational charts were in place the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system and the organizational charts were communicated to employees and updated in real time.	No exceptions noted.
		Inspected the company organizational charts and the company intranet to determine that organizational charts were in place and communicated to employees.	No exceptions noted.
CC1.1.2	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place to define the skills and knowledge levels required for the competence levels of particular jobs for each employment position sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2: Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security.			
CC1.2.1	Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. These charts are communicated to employees and updated in real time.	Inquired of the CTO regarding organizational management to determine that organizational charts were in place the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system and the organizational charts were communicated to employees and updated in real time.	No exceptions noted.
		Inspected the company organizational charts and the company intranet to determine that organizational charts were in place and communicated to employees.	No exceptions noted.
CC1.2.2	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place to define the skills and knowledge levels required for the competence levels of particular jobs for each employment position sampled.	No exceptions noted.
CC1.3: The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and provides resources necessary for personnel to fulfill their responsibilities.			
CC1.3.1	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place to define the skills and knowledge levels required for the competence levels of particular jobs for each employment position sampled.	No exceptions noted.
CC1.3.2	New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	Inspected the new employee hiring procedures to determine that new employee hiring procedures were in place to guide the hiring process and included verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.3	Employees are required to complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit policies.	Inquired of the information security manager regarding security awareness training to determine that employees were required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
		Inspected the security awareness training content and evidence of completion for a sample of employees hired during the review period to determine that security awareness training was completed for each employee sampled.	No exceptions noted.
		Inspected the security awareness training content and evidence of completion for a sample of current employees to determine that security awareness training was completed for each employee sampled during the 12 months preceding the end of the review period.	No exceptions noted.
CC1.3.4	Employees are required to sign a nondisclosure agreement upon hire.	Inspected the signed nondisclosure agreement for a sample of employees hired during the review period to determine that that employees were required to sign a nondisclosure agreement upon hire for each employee sampled.	No exceptions noted.
CC1.3.5	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.	Inspected available training courses to determine that training courses were available to new and existing employees to maintain and advance the skill level of personnel.	No exceptions noted.
CC1.3.6	Documented security policies and procedures are in place to communicate established workplace conduct standards, acceptable use, and information security policies, and conduct enforcement procedures to internal users. The security policies and procedures are communicated to employees via the corporate intranet site.	Inspected the security policies and procedures and the corporate intranet to determine that documented security policies and procedures were in place to communicate established workplace conduct standards, acceptable use, and information security policies, and conduct enforcement procedures to internal users and the policies and procedures were communicated to employees via the corporate intranet site.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.7	The entity's IT security group monitors the security impact of emerging technologies and the impact of applicable laws or regulations are considered by senior management.	Inquired of the CTO regarding the monitoring of threats and emergency technology to determine that the entity's IT security group monitored the security impact of emerging technologies and that the impact of applicable laws or regulations were considered by senior management.	No exceptions noted.
		Inspected security updates and notifications to determine that the entity's IT security group monitored the security impact of emerging technologies and the impact of applicable laws or regulations were considered by senior management.	No exceptions noted.
CC1.4: The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security.			
CC1.4.1	Documented security policies and procedures are in place to communicate established workplace conduct standards, acceptable use and information security policies, and conduct enforcement procedures to internal users. The security policies and procedures are communicated to employees via the corporate intranet site.	Inspected the security policies and procedures and the corporate intranet to determine that documented security policies and procedures were in place to communicate established workplace conduct standards, acceptable use and information security policies, and conduct enforcement procedures to internal users and the policies and procedures were communicated to employees via the corporate intranet site.	No exceptions noted.
CC1.4.2	Employees are required to sign an acknowledgment form upon hire indicating that they have been given access to the employment policies and understand their responsibility for adhering to the code of conduct outlined within the employment policies.	Inspected the employee policies and the signed acknowledgments for a sample of employees hired during the review period to determine that employees were required to sign an acknowledgement form upon hire indicating that they were given access to the employee manual and understood their responsibility for adhering to the code of conduct outlined within the employment policies for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.3	Employees are required to complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit policies.	Inquired of the information security manager regarding security awareness training to determine that employees were required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
		Inspected the security awareness training content and evidence of completion for a sample of employees hired during the review period to determine that security awareness training was completed for each employee sampled.	No exceptions noted.
		Inspected the security awareness training content and evidence of completion for a sample of current employees to determine that security awareness training was completed for each employee sampled during the 12 months preceding the end of the review period.	No exceptions noted.
CC1.4.4	Background checks are performed for employees working with customer data as a component of the hiring process.	Inspected the completed background check documentation for a sample of employees working with customer data hired during the review period to determine that background checks were performed as a component of the hiring process for each employee sampled.	No exceptions noted.
CC1.4.5	Employees are required to sign a nondisclosure agreement upon hire.	Inspected the signed nondisclosure agreement for a sample of employees hired during the review period to determine that that employees were required to sign a nondisclosure agreement upon hire for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.0: Common Criteria Related to Communications			
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 role in the system and the results of system operation.			
CC2.1.1	System policies and procedures are documented that include descriptions of the services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems. The policies and procedures are communicated to authorized internal and external users.	Inquired of the CTO regarding the system description to determine that system policies and procedures were documented that included descriptions of the services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems and that it was communicated to authorized internal and external users.	No exceptions noted.
		Inspected the description of services and the security policies and procedures and evidence of communication to determine that systems policies and procedures were documented and that they were communicated to authorized internal and external users.	No exceptions noted.
CC2.2: The entity's security 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.			
CC2.2.1	The entity's security commitments and the associated system requirements are documented in master subscription agreements.	Inspected the master subscription agreement template to determine that the entity's security commitments and the associated system requirements were documented in master subscription agreements.	No exceptions noted.
CC2.2.2	Employees are required to complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit policies.	Inquired of the information security manager regarding security awareness training to determine that employees were required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
		Inspected the security awareness training content and evidence of completion for a sample of employees hired during the review period to determine that security awareness training was completed for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the security awareness training content and evidence of completion for a sample of current employees to determine that security awareness training was completed for each employee sampled during the 12 months preceding the end of the review period.	No exceptions noted.
CC2.2.3	Employees are required to sign a nondisclosure agreement upon hire.	Inspected the signed nondisclosure agreement for a sample of employees hired during the review period to determine that that employees were required to sign a nondisclosure agreement upon hire for each employee sampled.	No exceptions noted.
CC2.2.4	Documented security policies and procedures are in place to communicate established workplace conduct standards, acceptable use, and information security policies, and conduct enforcement procedures to internal users. The security policies and procedures are communicated to employees via the corporate intranet site.	Inspected the security policies and procedures and the corporate intranet to determine that documented security policies and procedures were in place to communicate established workplace conduct standards, acceptable use, and information security policies, and conduct enforcement procedures to internal users and the policies and procedures were communicated to employees via the corporate intranet site.	No exceptions noted.
CC2.2.5	Employees are required to sign an acknowledgment form upon hire indicating that they have been given access to the employment policies and understand their responsibility for adhering to the code of conduct outlined within the employment policies.	Inspected the employee policies and the signed acknowledgments for a sample of employees hired during the review period to determine that employees were required to sign an acknowledgement form upon hire indicating that they were given access to the employee manual and understood their responsibility for adhering to the code of conduct outlined within the employment policies for each employee sampled.	No exceptions noted.
CC2.3: The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.			
CC2.3.1	Employees are required to complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit policies.	Inquired of the information security manager regarding security awareness training to determine that employees were required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the security awareness training content and evidence of completion for a sample of employees hired during the review period to determine that security awareness training was completed for each employee sampled.	No exceptions noted.
		Inspected the security awareness training content and evidence of completion for a sample of current employees to determine that security awareness training was completed for each employee sampled during the 12 months preceding the end of the review period.	No exceptions noted.
CC2.3.2	Documented security policies and procedures are in place to communicate established workplace conduct standards, acceptable use, and information security policies, and conduct enforcement procedures to internal users. The security policies and procedures are communicated to employees via the corporate intranet site.	Inspected the security policies and procedures and the corporate intranet to determine that documented security policies and procedures were in place to communicate established workplace conduct standards, acceptable use, and information security policies, and conduct enforcement procedures to internal users and the policies and procedures were communicated to employees via the corporate intranet site.	No exceptions noted.
CC2.3.3	Employees are required to sign an acknowledgment form upon hire indicating that they have been given access to the employment policies and understand their responsibility for adhering to the code of conduct outlined within the employment policies.	Inspected the employee policies and the signed acknowledgments for a sample of employees hired during the review period to determine that employees were required to sign an acknowledgement form upon hire indicating that they were given access to the employee manual and understood their responsibility for adhering to the code of conduct outlined within the employment policies for each employee sampled.	No exceptions noted.
CC2.3.4	The entity's security commitments and the associated system requirements are documented in master subscription agreements.	Inspected the master subscription agreement template to determine that the entity's security commitments and the associated system requirements were documented in master subscription agreements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.4: Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security of the system, is provided to personnel to carry out their responsibilities.			
CC2.4.1	Employees are required to complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit policies.	Inquired of the information security manager regarding security awareness training to determine that employees were required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
		Inspected the security awareness training content and evidence of completion for a sample of employees hired during the review period to determine that security awareness training was completed for each employee sampled.	No exceptions noted.
		Inspected the security awareness training content and evidence of completion for a sample of current employees to determine that security awareness training was completed for each employee sampled during the 12 months preceding the end of the review period.	No exceptions noted.
CC2.4.2	Documented security policies and procedures are in place to communicate established workplace conduct standards, acceptable use, and information security policies, and conduct enforcement procedures to internal users. The security policies and procedures are communicated to employees via the corporate intranet site.	Inspected the security policies and procedures and the corporate intranet to determine that documented security policies and procedures were in place to communicate established workplace conduct standards, acceptable use, and information security policies, and conduct enforcement procedures to internal users and the policies and procedures were communicated to employees via the corporate intranet site.	No exceptions noted.
CC2.4.3	Employees are required to sign an acknowledgment form upon hire indicating that they have been given access to the employment policies and understand their responsibility for adhering to the code of conduct outlined within the employment policies.	Inspected the employee policies and the signed acknowledgments for a sample of employees hired during the review period to determine that employees were required to sign an acknowledgement form upon hire indicating that they were given access to the employee manual and understood their responsibility for adhering to the code of conduct outlined within the employment policies for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.5: Internal and external users have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel.			
CC2.5.1	Documented escalation procedures for reporting security incidents and security vulnerabilities are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the security incident and security vulnerability escalation procedures to determine that documented escalation procedures for reporting security incidents and security vulnerabilities were provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC2.5.2	An online portal with phone numbers and a security e-mail is available to internal and external users to report security incidents and security vulnerabilities to Braze personnel.	Inspected the online portal for external users to determine that an online portal with phone numbers and a security e-mail was available to external users to report security incidents and security vulnerabilities to Braze personnel.	No exceptions noted.
CC2.6: System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security are communicated to those users in a timely manner.			
CC2.6.1	Change management meetings are held on at least a monthly basis to discuss and communicate the ongoing and upcoming changes and releases that affect the system.	Inspected the change management meeting agenda for a sample of months during the review period to determine that a change management meeting was held to discuss and communicate the ongoing changes and releases that affected the system for each month sampled.	No exceptions noted.
CC2.6.2	Release notes are documented and communicated to customers and internal personnel on at least a monthly basis to communicate changes and maintenance that affect system security.	Inspected the release notes for a sample of months to determine that release notes were documented and communicated to customers and internal personnel to communicate changes and maintenance that affected system security for each month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.0: Common Criteria Related to Risk Management and Design and Implementation of Controls			
CC3.1: The entity (1) identifies potential threats that could impair system security 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.			
CC3.1.1	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the risk assessment policy and most recent risk assessment performed to determine that a formal risk assessment was performed and that risks that were identified were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review during the 12 months preceding the end of the review period.	No exceptions noted.
CC3.1.2	The entity's IT security group monitors the security impact of emerging technologies and the impact of applicable laws or regulations are considered by senior management.	Inquired of the CTO regarding the monitoring of threats and emergency technology to determine that the entity's IT security group monitored the security impact of emerging technologies and that the impact of applicable laws or regulations were considered by senior management.	No exceptions noted.
		Inspected security updates and notifications to determine that the entity's IT security group monitored the security impact of emerging technologies and the impact of applicable laws or regulations were considered by senior management.	No exceptions noted.
CC3.2: The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.			
CC3.2.1	A third-party specialist performs an external penetration assessment on an annual basis to identify potential security vulnerabilities.	Inspected the most recent penetration test performed to determine that a third-party specialist performed an external penetration assessment to identify potential security vulnerabilities during the 12 months preceding the end of the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.2	A ticketing system is utilized to track, review, and remediate security vulnerabilities identified in the annual penetration tests.	Inspected the evidence of vulnerability tracking for a sample of security issues identified from the annual penetration test to determine that a ticketing system was utilized to track, review, and remediate security vulnerabilities identified in the annual penetration test for each vulnerability sampled.	No exceptions noted.
CC3.2.3	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the risk assessment policy and most recent risk assessment performed to determine that a formal risk assessment was performed and that risks that were identified were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review during the 12 months preceding the end of the review period.	No exceptions noted.
CC4.0: Common Criteria Related to Monitoring Controls			
CC4.1: The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.			
CC4.1.1	Documented escalation procedures for reporting security incidents and security vulnerabilities are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the security incident and security vulnerability escalation procedures to determine that documented escalation procedures for reporting security incidents and security vulnerabilities were provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC4.1.2	A third-party specialist performs an external penetration assessment on an annual basis to identify potential security vulnerabilities.	Inspected the results of the most recent penetration test to determine that a third-party specialist performed an external penetration assessment to identify potential security vulnerabilities during the 12 months preceding the end of the review period.	No exceptions noted.
CC4.1.3	A ticketing system is utilized to track, review, and remediate security vulnerabilities identified in the annual penetration tests.	Inspected the evidence of vulnerability tracking for a sample of security issues identified from the annual penetration test to determine that a ticketing system was utilized to track, review, and remediate security vulnerabilities identified in the annual penetration test for each vulnerability sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.4	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the risk assessment policy and most recent risk assessment performed to determine that a formal risk assessment was performed and that risks that were identified were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review during the 12 months preceding the end of the review period.	No exceptions noted.
CC5.0: Common Criteria Related to Logical and Physical Access Controls			
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.			
CC5.1.1	Documented information security policies and procedures are in place to govern information security standards.	Inspected the information security policies and procedures to determine that documented information security policies and procedures were in place to govern information security standards.	No exceptions noted.
CC5.1.2	A standard build script is utilized for installation and maintenance of production servers.	Inspected the standard build script to determine that a standard build script was utilized for installation and maintenance of production servers.	No exceptions noted.
CC5.1.3	User access requests to the production environment are documented within a ticketing system and require the approval of authorized management.	Inquired of the CTO regarding the provisioning process for production system access to determine that user access requests to the production environment were documented within a ticketing system and required the approval of authorized management.	No exceptions noted.
		Inspected the request ticket for a sample of user access requests processed during the review period to determine that user access requests to the production environment were documented within a ticketing system and required the approval of authorized management for each user access request sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.4	User access privileges to the in-scope systems are reviewed on a quarterly basis to help ensure that access is appropriate and that accounts assigned to terminated employees have been revoked.	Inspected the user access review for a sample of quarters during the review period to determine that user access privileges to the in-scope systems were reviewed to help ensure that access was appropriate and that accounts assigned to terminated employees had been revoked for each quarter sampled.	No exceptions noted.
CC5.1.5	Users are authenticated via an authorized user account and password before being granted access to the AWS and Rackspace portals.	Inspected the AWS and Rackspace portal login configurations to determine that users were authenticated via an authorized user account and password before being granted access to the AWS and Rackspace portals.	No exceptions noted.
CC5.1.6	Users are required to authenticate to the VPN via two-factor authentication.	Inspected the VPN authentication configuration to determine that users were required to authenticate to VPN via two-factor authentication.	No exceptions noted.
CC5.1.7	Users are required to authenticate with a valid user account and SSH private key pair before being granted access to the Linux server operating system.	Inspected the SSH configuration within the server management script and the login screen for an example production server to determine that users were required to authenticate with a valid user account and SSH private key pair before being granted access to the Linux server operating system.	No exceptions noted.
CC5.1.8	Users are required to authenticate with a valid user account and password before being granted access to the database.	Inspected the login configurations for a sample of databases to determine that users were authenticated via an authorized user account and password before being granted access to the database for each database sampled.	No exceptions noted.
CC5.1.9	Users are required to authenticate with a valid user account and password before being granted access to the application.	Inspect the application login configurations to determine that users were authenticated via an authorized user account and password before being granted access to the application.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.10	<p>Administrator access within the following in-scope systems is restricted to user accounts accessible by authorized personnel:</p> <ul style="list-style-type: none"> • AWS and Rackspace portals • Server operating system • Database • Application • VPN 	<p>Inspected user access listing with the assistance of the CTO to determine that administrator access to the following in-scope systems was restricted to user accounts accessible by authorized IT personnel:</p> <ul style="list-style-type: none"> • AWS and Rackspace portals • Server operating system • Database • Application • VPN 	No exceptions noted.
CC5.1.11	Remote access to the production environment is secured via encrypted VPN tunnels.	Inspected the VPN encryption configuration to determine that remote access to the production environment was secured via encrypted VPN tunnels.	No exceptions noted.
AWS and Rackspace are responsible for ensuring logical access to the underlying network, virtualization management, and storage devices for the IaaS and DBaaS services where Braze systems reside.			
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 granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC5.2.1	User access requests to the production environment are documented within a ticketing system and require the approval of authorized management.	Inquired of the CTO regarding the provisioning process for production system access to determine that user access requests to the production environment were documented within a ticketing system and required the approval of authorized management.	No exceptions noted.
		Inspected the request ticket for a sample of user access requests processed during the review period to determine that user access requests to the production environment were documented within a ticketing system and required the approval of authorized management for each user access request sampled.	No exceptions noted.
CC5.2.2	Users are authenticated via an authorized user account and password before being granted access to the AWS and Rackspace portals.	Inspected the AWS and Rackspace portal login configurations to determine that users were authenticated via an authorized user account and password before being granted access to the AWS and Rackspace portals.	No exceptions noted.
CC5.2.3	Users are required to authenticate to the VPN via two-factor authentication.	Inspected the VPN authentication configuration to determine that users were required to authenticate to VPN via two-factor authentication.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2.4	Users are required to authenticate with a valid user account and SSH private key pair before being granted access to the Linux server operating system.	Inspected the SSH configuration within the server management script and the login screen for an example production server to determine that users were required to authenticate with a valid user account and SSH private key pair before being granted access to the Linux server operating system.	No exceptions noted.
CC5.2.5	Users are required to authenticate with a valid user account and password before being granted access to the database.	Inspected the login configurations for a sample of databases to determine that users were authenticated via an authorized user account and password before being granted access to the database for each database sampled.	No exceptions noted.
CC5.2.6	Users are required to authenticate with a valid user account and password before being granted access to the application.	Inspect the application login configurations to determine that users were authenticated via an authorized user account and password before being granted access to the application.	No exceptions noted.
CC5.2.7	User privileges to in-scope systems that are assigned to terminated employees are revoked as a component of the employee termination process.	Inspected the termination checklist and the production environment user access listings for a sample of employees terminated during the review period to determine that user privileges to in-scope systems that were assigned to each terminated employee sampled were revoked as a component of the employee termination process for each terminated employee.	No exceptions noted.
CC5.2.8	User access privileges to the in-scope systems are reviewed on a quarterly basis to help ensure that access is appropriate and that accounts assigned to terminated employees have been revoked.	Inspected the user access review for a sample of quarters during the review period to determine that user access privileges to the in-scope systems were reviewed to help ensure that access was appropriate and that accounts assigned to terminated employees had been revoked for each quarter sampled.	No exceptions noted.
CC5.2.9	Remote access to the production environment is secured via encrypted VPN tunnels.	Inspected the VPN encryption configuration to determine that remote access to the production environment was secured via encrypted VPN tunnels.	No exceptions noted.
	AWS and Rackspace are responsible for ensuring logical access to the underlying network, virtualization management, and storage devices for the IaaS and DBaaS services where Braze systems reside.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC5.3.1	Users are authenticated via an authorized user account and password before being granted access to the AWS and Rackspace portals.	Inspected the AWS and Rackspace portal login configurations to determine that users were authenticated via an authorized user account and password before being granted access to the AWS and Rackspace portals.	No exceptions noted.
CC5.3.2	Users are required to authenticate to the VPN via two-factor authentication.	Inspected the VPN authentication configuration to determine that users were required to authenticate to VPN via two-factor authentication.	No exceptions noted.
CC5.3.3	Users are required to authenticate with a valid user account and SSH private key pair before being granted access to the Linux server operating system.	Inspected the SSH configuration within the server management script and the login screen for an example production server to determine that users were required to authenticate with a valid user account and SSH private key pair before being granted access to the Linux server operating system.	No exceptions noted.
CC5.3.4	Users are required to authenticate with a valid user account and password before being granted access to the database.	Inspected the login configurations for a sample of databases to determine that users were authenticated via an authorized user account and password before being granted access to the database for each database sampled.	No exceptions noted.
CC5.3.5	Users are required to authenticate with a valid user account and password before being granted access to the application.	Inspect the application login configurations to determine that users were authenticated via an authorized user account and password before being granted access to the application.	No exceptions noted.
CC5.3.6	Remote access to the production environment is secured via encrypted VPN tunnels.	Inspected the VPN encryption configuration to determine that remote access to the production environment was secured via encrypted VPN tunnels.	No exceptions noted.
AWS and Rackspace are responsible for ensuring logical access to the underlying network, virtualization management, and storage devices for the IaaS and DBaaS services where Braze systems reside.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC5.4.1	User access requests to the production environment are documented within a ticketing system and require the approval of authorized management.	Inquired of the CTO regarding the provisioning process for production system access to determine that user access requests to the production environment were documented within a ticketing system and required the approval of authorized management.	No exceptions noted.
		Inspected the request ticket for a sample of user access requests processed during the review period to determine that user access requests to the production environment were documented within a ticketing system and required the approval of authorized management for each user access request sampled.	No exceptions noted.
CC5.4.2	User privileges to in-scope systems that are assigned to terminated employees are revoked as a component of the employee termination process.	Inspected the termination checklist and the production environment user access listings for a sample of employees terminated during the review period to determine that user privileges to in-scope systems that were assigned to each terminated employee sampled were revoked as a component of the employee termination process for each terminated employee.	No exceptions noted.
CC5.4.3	User access privileges to the in-scope systems are reviewed on a quarterly basis to help ensure that access is appropriate and that accounts assigned to terminated employees have been revoked.	Inspected the user access review for a sample of quarters during the review period to determine that user access privileges to the in-scope systems were reviewed to help ensure that access was appropriate and that accounts assigned to terminated employees had been revoked for each quarter sampled.	No exceptions noted.
	AWS and Rackspace are responsible for ensuring logical access to the underlying network, virtualization management, and storage devices for the IaaS and DBaaS services where Braze systems reside.		
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.			
CC5.5.1	Third-party vendors are reviewed on an annual basis to help ensure that they are meeting Braze commitments and system requirements as they relate to security.	Inspected evidence of completed third-party vendor reviews to determine that third-party vendors were reviewed on an annual basis to help ensure that they were meeting Braze commitments and system requirements as they relate to security.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	AWS and Rackspace are responsible for ensuring controls for restricting physical access to data center facilities, backup media, and other system components including network devices, virtualization, and storage infrastructure.		
CC5.6: Logical access security measures have been implemented to protect against security threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.			
CC5.6.1	A firewall utility is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagrams and firewall system configurations to determine that a firewall utility was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
CC5.6.2	The firewall utility is configured to deny any type of network connection that is not explicitly authorized by a firewall rule.	Inspected the firewall system configurations to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall.	No exceptions noted.
CC5.6.3	Externally routable IP addresses are not assigned to internal production servers. Network address translation (NAT) functionality of the firewall utility is configured to manage internal IP addresses.	Inspected the network diagrams and firewall system configurations to determine that externally routable IP addresses were not assigned to internal production servers and that NAT functionality of the firewall utility was configured to manage internal IP addresses.	No exceptions noted.
CC5.6.4	A third-party specialist performs an external penetration assessment on an annual basis to identify potential security vulnerabilities.	Inspected the most recent penetration test performed to determine that a third-party specialist performed an external penetration assessment to identify potential security vulnerabilities during the 12 months preceding the end of the review period.	No exceptions noted.
CC5.6.5	Web sessions are encrypted using TLS encryption protocol.	Inspected the web session encryption configurations to determine that web servers utilized TLS encryption for web communication sessions.	No exceptions noted.
CC5.6.6	Remote access to the production environment is secured via encrypted VPN tunnels.	Inspected the VPN encryption configuration to determine that remote access to the production environment was secured via encrypted VPN tunnels.	No exceptions noted.
	AWS and Rackspace are responsible for ensuring logical access to the underlying network, virtualization management, and storage devices for the IaaS and DBaaS services where Braze systems reside.		
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.			
CC5.7.1	Policies are in place that prohibit the transmission of sensitive information over the internet or other public communications paths unless it is encrypted.	Inspected the encryption policies to determine that policies were in place that prohibit the transmission of sensitive information over the internet or other public communications paths unless it was encrypted.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.7.2	Remote access to the production environment is secured via encrypted VPN tunnels.	Inspected the VPN encryption configuration to determine that remote access to the production environment was secured via encrypted VPN tunnels.	No exceptions noted.
CC5.7.3	Web sessions are encrypted using TLS encryption protocol.	Inspected the web session encryption configurations to determine that web servers utilized TLS encryption for web communication sessions.	No exceptions noted.
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.			
CC5.8.1	Employees are required to complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit policies.	Inquired of the information security manager regarding security awareness training to determine that employees were required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
		Inspected the security awareness training content and evidence of completion for a sample of employees hired during the review period to determine that security awareness training was completed for each employee sampled.	No exceptions noted.
CC5.8.2	Documented security policies and procedures are in place to communicate established workplace conduct standards, acceptable use, and information security policies, and conduct enforcement procedures to internal users. The security policies and procedures are communicated to employees via the corporate intranet site.	Inspected the security policies and procedures and the corporate intranet to determine that documented security policies and procedures were in place to communicate established workplace conduct standards, acceptable use, and information security policies, and conduct enforcement procedures to internal users and the policies and procedures were communicated to employees via the corporate intranet site.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.8.3	Employees are required to sign an acknowledgment form upon hire indicating that they have been given access to the employment policies and understand their responsibility for adhering to the code of conduct outlined within the employment policies.	Inspected the employee policies and the signed acknowledgments for a sample of employees hired during the review period to determine that employees were required to sign an acknowledgement form upon hire indicating that they were given access to the employee manual and understood their responsibility for adhering to the code of conduct outlined within the employment policies for each employee sampled.	No exceptions noted.
	AWS and Rackspace are responsible for the implementation of controls to prevent, detect, and act upon incidents, security breaches, and unauthorized/malicious software on the IaaS and DBaaS systems that support the Braze Services system.		
CC6.0: Common Criteria Related to System Operations			
CC6.1: Vulnerabilities of system components to security 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.			
CC6.1.1	A firewall utility is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagrams and firewall system configurations to determine that a firewall utility was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
CC6.1.2	The firewall utility is configured to deny any type of network connection that is not explicitly authorized by a firewall rule.	Inspected the firewall system configurations to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall.	No exceptions noted.
CC6.1.3	Externally routable IP addresses are not assigned to internal production servers. NAT functionality of the firewall utility is configured to manage internal IP addresses.	Inspected the network diagrams and firewall system configurations to determine that externally routable IP addresses were not assigned to internal production servers and that NAT functionality of the firewall utility was configured to manage internal IP addresses.	No exceptions noted.
CC6.1.4	A third-party specialist performs an external penetration assessment on an annual basis to identify potential security vulnerabilities.	Inspected the most recent penetration test performed to determine that a third-party specialist performed an external penetration assessment to identify potential security vulnerabilities during the 12 months preceding the end of the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.5	A ticketing system is utilized to track, review, and remediate security vulnerabilities identified in the annual penetration tests.	Inspected the evidence of vulnerability tracking for a sample of security issues identified from the annual penetration test to determine that a ticketing system was utilized to track, review, and remediate security vulnerabilities identified in the annual penetration test for each vulnerability sampled.	No exceptions noted.
CC6.2: Security 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.			
CC6.2.1	Documented escalation procedures for reporting security incidents and security vulnerabilities are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the security incident and security vulnerability escalation procedures to determine that documented escalation procedures for reporting security incidents and security vulnerabilities were provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC6.2.2	An online portal with phone numbers and a security e-mail is available to internal and external users to report security incidents and security vulnerabilities to Braze personnel.	Inspected the online portal for external users to determine that an online portal with phone numbers and a security e-mail was available to external users to report security incidents and security vulnerabilities to Braze personnel.	No exceptions noted.
CC6.2.3	Management meetings are held on at least a monthly basis to discuss incidents and corrective measures to help ensure that incidents are resolved and what steps can be taken to prevent further incidents.	Inspected the management meeting agenda for a sample of months during the review period to determine that management meetings were held to discuss incidents and corrective measures to help ensure that incidents were resolved and what steps could be taken to prevent further incidents for each month sampled.	No exceptions noted.
CC6.2.4	A ticketing system is utilized to track security incidents through resolution.	Inspected the ticketing system and a ticket for an example security incident resolved during the review period to determine that a ticketing system was utilized to track security incidents through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.5	Employees are required to complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit policies.	Inquired of the information security manager regarding security awareness training to determine that employees were required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
		Inspected the security awareness training content and evidence of completion for a sample of employees hired during the review period to determine that security awareness training was completed for each employee sampled.	No exceptions noted.
		Inspected the security awareness training content and evidence of completion for a sample of current employees to determine that security awareness training was completed for each employee sampled during the 12 months preceding the end of the review period.	No exceptions noted.
CC6.2.6	Documented security policies and procedures are in place to communicate established workplace conduct standards, acceptable use and information security policies, and conduct enforcement procedures to internal users. The security policies and procedures are communicated to employees via the corporate intranet site.	Inspected the security policies and procedures and the corporate intranet to determine that documented security policies and procedures were in place to communicate established workplace conduct standards, acceptable use and information security policies, and conduct enforcement procedures to internal users and the policies and procedures were communicated to employees via the corporate intranet site.	No exceptions noted.
CC7.0: Common Criteria Related to Change Management			
CC7.1: The entity's commitments and system requirements, as they relate to security, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.			
CC7.1.1	Documented policies and procedures are in place to guide personnel in performing change management procedures.	Inspected the change management policies and procedures to determine that documented policies and procedures were in place to guide personnel in performing change management procedures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.2	Change management meetings are held on at least a monthly basis to discuss and communicate the ongoing and upcoming changes and releases that affect the system.	Inspected the change management meeting agenda for a sample of months during the review period to determine that a change management meeting was held to discuss and communicate the ongoing changes and releases that affected the system for each month sampled.	No exceptions noted.
CC7.1.3	A change management ticketing system is utilized to centrally maintain, manage, and monitor enhancement, development, and maintenance activities.	Inspected the change management ticket for a sample of changes during the review period to determine that a change management ticketing system was utilized to centrally maintain, manage, and monitor enhancement, development, and maintenance activities for each change selected.	No exceptions noted.
CC7.1.4	A version control system is utilized to control access to source code and to track change activities.	Inspected evidence of the version control system to determine that a version control system was utilized to control access to source code and to track change activities.	No exceptions noted.
CC7.1.5	QA testing is required to be performed on changes prior to merging them to the master branch.	Inquired of the CTO regarding QA testing to determine that QA testing was required to be performed on changes prior to merging them to the master branch.	No exceptions noted.
		Inspected the QA testing for a sample of changes during the review period to determine that QA testing was required to be performed on changes that were merged to the master branch for each change sampled.	No exceptions noted.
CC7.1.6	Approval is required for changes that are pulled to the production branch prior to implementation.	Inquired of the CTO regarding the change management process to determine that approval was required for changes that were pulled to the production branch prior to implementation.	No exceptions noted.
		Inspected the change ticket for a sample of changes during the review period to determine that approval was obtained for each change sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.7	CI tests are configured to automatically run upon merging code from the development branch to the master branch. If the CI test fails, an e-mail is sent to the members involved in the change.	Inspected the CI test configurations and an example e-mail notification generated during the review period to determine that CI tests were configured to automatically run upon merging code from the development branch to the master branch and that if the CI test failed, an e-mail was sent to members involved in the change.	No exceptions noted.
CC7.1.8	Application development and testing efforts are performed in development environments that are logically separate from the production environment.	Inspected the server environments and IP address assignments to determine that application development and testing efforts were performed in development environments that were logically separate from the production environment.	No exceptions noted.
CC7.1.9	The ability to pull a change to the master branch is restricted to user accounts accessible by authorized IT personnel.	Inspected the listing of users with the ability to commit a change to the master branch with the assistance of the CTO to determine that the ability to pull a change to the master branch was restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
CC7.1.10	The ability to deploy a change to the production environment is restricted to user accounts accessible by authorized IT personnel.	Inspected the listing of users with the ability to deploy a change to the production environment with the assistance of the CTO to determine that the ability to deploy a change to the production environment was restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
CC7.1.11	Emergency changes requiring administrator override within the deployment tool are approved by another developer within 24 hours of change deployment.	Inspected the change ticket and evidence of review and approval for a sample of emergency change overrides during the review period to determine that emergency changes requiring administrator override within the deployment tool were approved by another developer within 24 hours of change deployment for each emergency change sampled.	No exceptions noted.
CC7.1.12	Release notes are documented and communicated to customers and internal personnel on at least a monthly basis to communicate changes and maintenance that affect system security.	Inspected the release notes for a sample of months to determine that release notes were documented and communicated to customers and internal personnel to communicate changes and maintenance that affected system security for each month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2: Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security.			
CC7.2.1	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the risk assessment policy and most recent risk assessment performed to determine that a formal risk assessment was performed and that risks that were identified were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review during the 12 months preceding the end of the review period.	No exceptions noted.
CC7.2.2	Management meetings are held on at least a monthly basis to discuss incidents and corrective measures to help ensure that incidents are resolved and what steps can be taken to prevent further incidents.	Inspected the management meeting agenda for a sample of months during the review period to determine that management meetings were held to discuss incidents and corrective measures to help ensure that incidents were resolved and what steps could be taken to prevent further incidents for each month sampled.	No exceptions noted.
CC7.2.3	A third-party specialist performs an external penetration assessment on an annual basis to identify potential security vulnerabilities.	Inspected the most recent penetration test performed to determine that a third-party specialist performed an external penetration assessment to identify potential security vulnerabilities during the 12 months preceding the end of the review period.	No exceptions noted.
CC7.2.4	A ticketing system is utilized to track, review, and remediate security vulnerabilities identified in the annual penetration tests.	Inspected the evidence of vulnerability tracking for a sample of security issues identified from the annual penetration test to determine that a ticketing system was utilized to track, review, and remediate security vulnerabilities identified in the annual penetration test for each vulnerability sampled.	No exceptions noted.
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.			
CC7.3.1	Management meetings are held on at least a monthly basis to discuss incidents and corrective measures to help ensure that incidents are resolved and what steps can be taken to prevent further incidents.	Inspected the management meeting agenda for a sample of months during the review period to determine that management meetings were held to discuss incidents and corrective measures to help ensure that incidents were resolved and what steps could be taken to prevent further incidents for each month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3.2	Documented escalation procedures for reporting security incidents and security vulnerabilities are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the security incident and security vulnerability escalation procedures to determine that documented escalation procedures for reporting security incidents and security vulnerabilities were provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC7.4: Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security commitments and system requirements.			
CC7.4.1	A change management ticketing system is utilized to centrally maintain, manage, and monitor enhancement, development, and maintenance activities.	Inspected the change management ticket for a sample of changes during the review period to determine that a change management ticketing system was utilized to centrally maintain, manage, and monitor enhancement, development, and maintenance activities for each change selected.	No exceptions noted.
CC7.4.2	QA testing is required to be performed on changes prior to merging them to the master branch.	Inquired of the CTO regarding QA testing to determine that QA testing was required to be performed on changes prior to merging them to the master branch.	No exceptions noted.
		Inspected the QA testing for a sample of changes during the review period to determine that QA testing was required for changes that were pulled to the production branch prior to implementation for each change sampled.	No exceptions noted.
CC7.4.3	CI tests are configured to automatically run upon merging code from the development branch to the master branch. If the CI test fails, an e-mail is sent to the members involved in the change.	Inspected the CI test configurations and an example e-mail notification generated during the review period to determine that CI tests were configured to automatically run upon merging code from the development branch to the master branch and that if the CI test failed, an e-mail was sent to members involved in the change.	No exceptions noted.
CC7.4.4	Approval is required for changes that are pulled to the production branch prior to implementation.	Inquired of the CTO regarding the change management process to determine that approval was required for changes that were pulled to the production branch prior to implementation.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the change ticket for a sample of changes during the review period to determine that approval was required for changes that were pulled to the production branch prior to implementation for each change ticket sampled.	No exceptions noted.
CC7.4.5	Application development and testing efforts are performed in development environments that are logically separate from the production environment.	Inspected the server environments and IP address assignments to determine that application development and testing efforts were performed in development environments that were logically separate from the production environment.	No exceptions noted.
CC7.4.6	The ability to pull a change to the master branch is restricted to user accounts accessible by authorized IT personnel.	Inspected the listing of users with the ability to commit a change to the master branch with the assistance of the CTO to determine that the ability to pull a change to the master branch was restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
CC7.4.7	The ability to deploy a change to the production environment is restricted to user accounts accessible by authorized IT personnel.	Inspected the listing of users with the ability to deploy a change to the production environment with the assistance of the CTO to determine that the ability to deploy a change to the production environment was restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
CC7.4.8	Emergency changes requiring administrator override within the deployment tool are approved by another developer within 24 hours of change deployment.	Inspected the change ticket and evidence of review and approval for a sample of emergency change overrides during the review period to determine that emergency changes requiring administrator override within the deployment tool were approved by another developer within 24 hours of change deployment for each emergency change sampled.	No exceptions noted.
CC7.4.9	Release notes are documented and communicated to customers and internal personnel on at least a monthly basis to communicate changes and maintenance that affect system security.	Inspected the release notes for a sample of months to determine that release notes were documented and communicated to customers and internal personnel to communicate changes and maintenance that affected system security for each month sampled.	No exceptions noted.