betterworks®

Report on Betterworks' Goal Setting & Continuous Performance Management Platform Relevant to Security, Availability, Confidentiality, and Privacy (SOC 3 Report)

For the *Period March 1, 2018 to February 28, 2019*

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations ™

THE
cadence
GROUP

THE cadence GROUP

O 801.349.1360
F 866.326.6612

PO Box 711190
Salt Lake City, Utah 84171
www.thecadencegroup.com

Section I – Report of Independent Service Auditors

To: Betterworks Systems, Inc.

We have examined management's assertion that Betterworks maintained effective controls to provide reasonable assurance that:

- the Betterworks Goal Setting & Continuous Performance Management Platform was protected against unauthorized access, use, or modification to achieve Betterworks' service commitments and system requirements
- the Betterworks Goal Setting & Continuous Performance Management Platform was available for operation and use to achieve Betterworks' service commitments and system requirements
- the Betterworks Goal Setting & Continuous Performance Management Platform information is collected, used, disclosed, and retained to achieve Betterworks' service commitments and system requirements
- personal information within the Betterworks Goal Setting & Continuous Performance Management Platform is collected, used, disclosed, and retained to achieve Betterworks' service commitments and system requirements

during the period March 1, 2018 to February 28, 2019 based on the criteria for Security, Availability, Confidentiality, and Privacy set forth in the TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). This assertion is the responsibility of Betterworks' management. Our responsibility is to express an opinion based on our examination.

Betterworks is responsible for its service commitments and system requirements and for designing, implementing, operating, and maintaining effective controls within the Goal Setting & Continuous Performance Management Platform to provide reasonable assurance that Betterworks' service commitments and system requirements were achieved. Betterworks has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Betterworks is responsible for selecting and identifying in its assertion the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated. An examination involves performing procedures to obtain evidence about management's assertion, which includes (1) obtaining an understanding of Betterworks' relevant security, availability, confidentiality, and privacy controls, (2) Assessing the risks that controls were not effective to achieve Betterworks' service commitments and system requirements based on the applicable trust services criteria, and (3) performing procedures to obtain evidence about whether controls within the system were effective to achieve Betterworks' service commitments and system requirements based the applicable trust services criteria, and (4) performing such other procedures as we considered necessary. We believe that our examination provides a reasonable basis for our opinion.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

During the period under review, Betterworks used multiple sub-service providers; Amazon Web Services (AWS) for the management and hosting of production servers (in an Infrastructure as a Service model), Heroku to host the platform within the production environment (in a Platform as a Service model), and Box to securely transmit and store customer-specific documents used in customizing the Betterworks Services for each customer. Consequently, certain controls are the responsibility of AWS, Heroku, and Box, and are not included within the scope of this examination.

Betterworks' assertion also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls contemplated in the design of Betterworks' controls are suitably designed and operating effectively, along with related controls at Betterworks. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Opinion

In our opinion, Betterworks' management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, confidentiality, and privacy.

Cadence Assurance LLC

Salt Lake City, Utah
April 3, 2019

Section II – Betterworks' Assertion Regarding the Effectiveness of Its Controls over the Goal Setting & Continuous Performance Management Platform

We, as management of Betterworks, are responsible for designing, implementing, operating, and maintaining effective controls over the Betterworks Goal Setting & Continuous Performance Management Platform (Platform) to provide reasonable assurance that the service commitments and system requirements related to security, availability, confidentiality, and privacy were achieved.

We have performed an evaluation of the effectiveness of the controls over the Platform throughout the period March 1, 2018 to February 28, 2019, to achieve the service commitments and system requirements related to the operation of the Platform using the criteria for security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in the TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Based on this evaluation and the applicable trust services criteria, we assert that the controls were effective throughout the period March 1, 2018 to February 28, 2019 to provide reasonable assurance that:

- the Betterworks Goal Setting & Continuous Performance Management Platform was protected against unauthorized access, use or modification to achieve Betterworks' service commitments and system requirements
- the Betterworks Goal Setting & Continuous Performance Management Platform was available for operation and use to achieve Betterworks' service commitments and system requirements
- the Betterworks Goal Setting & Continuous Performance Management Platform information is collected, used, disclosed, and retained to achieve Betterworks' service commitments and system requirements
- personal information within the Betterworks Goal Setting & Continuous Performance Management Platform is collected, used, disclosed, and retained to achieve Betterworks' service commitments and system requirements

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

Betterworks uses multiple subservice organizations in conjunction with providing its Goal Setting & Continuous Performance Management Platform. Betterworks utilizes Amazon Web Services (AWS), which is used for management and hosting of the production servers (in an Infrastructure as a Service model). Heroku is used to host the platform within the production environment (in a Platform as a Service model). Box.com is used to securely transmit and store customer-specific documents used in customizing the Betterworks Services for each customer. The Description also indicates that certain trust services criteria specified therein can be met only if these subservice organizations' controls contemplated in the design of Betterworks' controls are suitably designed and operating effectively along with related controls at Betterworks. Testing procedures do not extend to controls of these subservice organizations.

The Description also indicates that certain trust services criteria specified in the Description can be met only in complementary user entity controls contemplated in the design of Betterworks' controls are suitably designed and operating effectively, along with related controls at Betterworks. Testing procedures do not extend to controls of user entities.

We assert that the controls within the Platform were effective throughout the period March 1, 2018 to February 28, 2019, to provide reasonable assurance that Betterworks' service commitments and system requirements were achieved based on the applicable trust services criteria.

Betterworks Systems, Inc.
April 3, 2019

Section III – Description of Betterworks' Goal Setting & Continuous Performance Management Platform

Company Overview

Betterworks is the solution of choice for forward-thinking HR and organizational leaders looking to motivate and engage their workforce to achieve today's business goals and tomorrow's challenges. The Betterworks software suite delivers goal transparency and alignment alongside the necessary, meaningful, ongoing conversations between managers and employees on progress, recognition, and development. Through an award-winning user experience and integrations with popular team productivity tools (Slack, Jira, Asana) and back-office HRIS (Workday, SuccessFactors), Betterworks makes rollout, administration, and end user adoption a breeze.

System Description

The Betterworks software suite includes the following features:

- *Conversations:* Manages check-ins, performance assessments, and employee reviews in one location, and guides employees through the process of answering question prompts, submitting and sharing responses, and confirming employee-manager meetings.
- *Peer Feedback:* Manages employee feedback, from scheduled end of year 360-degree feedback to employee-driven anytime feedback requests.
- *Goal Alignment:* Provides a goal-tracking platform supports employee, team, and company goal setting with advanced alignment, progress tracking, and software integrations.
- *Recognition:* Creates a centralized place for public positive and personalized recognition by peers and managers alike.
- *People Analytics:* Establishes advanced analytics for tracking your workforce as they move through your feedback and review processes.
- *Pulse:* Offers the ability to easily survey employees for up to the minute insights into needs, sentiment, and engagement.
- *HR Administration:* Allows HR program leaders have control over user administration, program design, calendarization, as well as customizable elements within the software.

Subservice Organizations

Betterworks uses the following subservice organizations in conjunction with providing its continuous performance management platform:

- *Amazon Web services (AWS)* is used to support the Betterworks production environment. AWS provides a secure infrastructure for compute power, storage, and other application services over the Internet.
- *Heroku* is used to provide application containers and database services.
- *Box* is used to securely store confidential and private information.

The BetterWorks Platform uses these subservice organizations to provide high availability and fault tolerance for the application. BetterWorks reviews the available SOC reports or other available information on a frequent basis (no less than once per year) to determine the effectiveness of these organizations' controls. This report excludes control objectives and related controls for services provided by the noted subservice organizations.

Principle Service Commitments and System Requirements

Betterworks designs its processes and procedures to provide and secure customer data. Betterworks' security commitments are documented and communicated to customers in service agreements, addendums, and at other resources as referenced below:

- Security Data Sheet (https://www.betterworks.com/security-datasheet/)
- Service Level Agreement (https://www.betterworks.com/sla/)
- Privacy Notice (https://www.betterworks.com/privacy-notice/)

System Components

The components of the Betterworks Platform include the following infrastructure, software, people, procedures, and data elements.

Infrastructure

The Betterworks software is available via a public cloud infrastructure. Web clients and the mobile application send and receive data via encrypted connections. The platform uses Amazon Web Services, AWS (infrastructure-as-a-service) services, and Heroku (platform-as-a-service, owned by Salesforce.com), which provide high-availability and fault-tolerance for the systems serving the application. The Betterworks application is served from load-balanced infrastructure, so adding additional resources is quick and seamless. During high loads, the platform can easily add additional application containers to serve simultaneous requests. During hardware or network failures, new devices are brought online to replace the faulty equipment.

Betterworks has implemented a multi-tenant architecture, which allows Betterworks to easily scale resources to meet demand, optimize performance, provide world-class service, and efficiently deploy upgrades with new features and security improvements. Data is attributed to a customer for each database row and cross dependencies are enforced with foreign key relations, further ensuring data integrity. This helps enforce record-level access control for all rows and database queries.

Platform infrastructure includes development, test, and staging environments, which are completely separate from the production environment.

Software

Betterworks maintains a library of open source projects in use. The production environment runs on Linux-based systems and is primarily developed in Python and JavaScript. Betterworks uses software to automatically test production code changes and securely deploy to production environments. Software is also used to monitor production environments for unauthorized use, errors, and performance.

People

Executive Management

In addition to managing business operations, executive management is ultimately responsible for the final determination of risk acceptance or mitigation. The executive management group is comprised of the most senior owners of information security risk in the company (the "Security Council").

With respect to information security, the role of executive management is to consistently demonstrate leadership and commitment to the program, its objectives, goals, enforcement, and continual improvement.

Employees

Support for the related controls, policies, and procedures come from the personnel involved in the development, operation, and support of the Betterworks Platform. These personnel include employees of the following departments:

- *Engineering*—Builds and tests new software tools and features that comprise and support the Betterworks Platform;
- *Product*—Designs and prioritizes changes to the Betterworks Platform;
- *Customer Success & Support*—Delivers successful customer deployments by educating customers about goal setting and how to use the Betterworks Platform, and responding to questions and customer issues;
- *People Operations*—Ensures Betterworks has the human capital resources for each function to deliver full support of the Betterworks Platform.

Procedures

Betterworks has an established information security organization managed by its internal Security Council. The Security Council establishes and maintains formal policies and procedures pertaining to security, availability, confidentiality, and privacy.

For BetterWorks, security is not just a product feature; it is a company initiative. Securing customer data and protecting customers is critical to the BetterWorks corporate mission. BetterWorks helps employees and managers work together in a secure, transparent and protected environment.

Each Betterworks policy is assigned an owner, reviewed, and approved as needed (no less than annually) by various members of the Security Council, and published to the Betterworks team. Relevant security, availability, confidentiality, and privacy policies are in place with regards to Betterworks' Goal Setting & Continuous Performance Management Platform. These policies are summarized below:

- Information Security Policy
- Organization of Information Security
- Mobile Devices and Teleworking
- Human Resources Security
- Asset Management
- Information Classification
- Media Handling
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisitions, Development and Maintenance

- Supplier Relationships
- Information Security Incident Management
- Information Security Aspects of Business Continuity Management
- Compliance

It is Betterworks' policy to protect the confidentiality, integrity, and availability of the information stored in any form. Betterworks information security practices must meet the standard of due care that is reasonably expected by customers, shareholders, partners, employees, and the business itself. Betterworks must also comply with laws and regulatory requirements where it does business. To this end, Betterworks maintains an information security program that:

- Exhibits top management's commitment to, and support of, information security
- Establishes information security policies and prioritized action plans
- Aligns with customer information security requirements and contractual information security obligations
- Delivers a consistent, documented information security risk management process
- Cultivates a sustainable, continuously improving program aligned to Betterworks' strategic priorities

Data

Customers retain sole and exclusive ownership of all customer data. "Customer Data" means confidential or proprietary data supplied by customers ("Customers") or end users of customers ("Users") to Betterworks through the use of the Betterworks Platform.

Internal Control Framework

Betterworks has adopted the following control framework to meet its security, availability, confidentiality, and privacy commitments. This framework includes the following aspects: control environment, risk assessment, control activities, information and communication, and monitoring.

Control Environment

Betterworks' internal control environment reflects the overall attitude, awareness, and actions of the board of directors, executive management, and other key stakeholders concerning the importance of controls and the emphasis given to controls in Betterworks' policies, procedures, methods, and organizational structure.

The Betterworks executive management team is responsible for directing and controlling operations, and for establishing, communicating, and monitoring policies and procedures. Importance is placed on maintaining sound internal controls and establishing the integrity and ethical values of personnel. Additionally, the executive management team meets with the board of directors to review company growth and performance, assess regulations and requirements, and monitor risk management activities.

The Betterworks organizational structure outlines responsibilities related to system availability and aligns personnel in a reporting structure that includes members of the Security Council. Established codes of conduct and security awareness are a part of employee training. Customer information availability commitments are communicated internally to employees and externally to customers.

Risk Assessment

Betterworks recognizes that risk management is a critical component of its operations that helps to verify that customer assets are properly protected. Betterworks management conducts periodic formal risk assessments. The ISMS Risk Assessment procedure document provides direction and training to managers, employees, and contractors responsible for facilitating these risk assessments to help ensure a consistent approach. The risk assessment process allows management to validate threats and investigate potential vulnerabilities to more effectively make decisions and assign resources to the mitigation of risk.

The result of a completed risk assessment is a Risk Treatment Plan. The Risk Treatment Plan records commitment to modify a risk by some combination of mitigating controls, modifying the system to avoid risk, and accepting the residual risk after treatment. A Risk Treatment Plan has a risk owner, a driver to ensure the work occurs, and a target completion date.

Betterworks considers the impact to data availability when assessing risk from various sources. The policies and procedures in place are consequently designed to address identified risks to data availability.

Management addresses and manages the risks inherent in the company's operations and implements procedures to monitor and mitigate these risks. The foundation of this process is management's knowledge of its operations, its close working relationship with its customers and vendors, and its understanding of the technology space in which it operates. Managers discuss and resolve issues as they arise within their groups, and monitor and adjust the control processes for which they are responsible on an as-needed basis. This process is monitored through both regularly scheduled meetings and other informal interactions.

Vendor Management

Betterworks uses AWS, Heroku, and Box subservice organizations in conjunction with providing its continuous performance management platform. Betterworks reviews the available SOC reports or other available information on a frequent basis (no less than once per year) to determine the effectiveness of these organizations' controls.

Control Activities

Controls have been established to ensure key processes operate as intended. These activities are designed to address both the relevant business risks and the underlying infrastructure relevant to the Betterworks Platform. The control activities are integrated into the policies and procedures outlined in the *Procedures* section above.

System Inventory

Betterworks maintains an asset inventory of systems including endpoints, production systems, and owners.

User Authentication

Betterworks systems are utilized to positively identify, authorize, and authenticate personnel before they are granted access to company information resources. Multi-factor authentication is required to access production systems.

Customers have the option to configure end users to authenticate using either a username and password, or integration with Single-Sign-On (SSO) through Google OAuth or SAML2.

Network Security

Heroku's containers provide a managed network and operating system configuration and prevent Betterworks employees from having root-level access. These containers, housing the customer-facing application components and associated databases, are restricted and centrally controlled. These restrictions include port restriction, allowing for only a single port to be open; an ephemeral file system that resets every 24 hours; disallowed root access; and no access to the operating system.

Encryption

Data stored in the Betterworks platform is encrypted using the AES-256 encryption algorithm. Data in transit is encrypted using SFTP and HTTPS for uploads of user information, and HTTPS using TLS 1.2 for web requests.

Additionally, full disk encryption is configured on company-owned laptops and mobile devices.

User Provisioning and Deprovisioning

Access permissions are limited to the minimum necessary to perform the assigned duties. Access to information resources is controlled through a defined and managed process which addresses authorizing, modifying, and revoking access, and which includes review of information system privileges. During the onboarding of new hires, access to systems is provisioned based on employee roles. Internal system access for terminated employees and contractors is removed within three business days from their termination dates.

Customer user accounts are provisioned, modified, and deprovisioned by company administrators. Betterworks works with Customers during the initial roll out to guide company administrators through the account provisioning process.

Antivirus

Company laptops are configured with antivirus software including real-time updates and on-access scanning.

Configuration Management

A configuration management tool is used to manage servers in the production environment. Access to the configuration management tool is restricted to IT Operations personnel. Significant infrastructure changes require testing and approval prior to implementation to production.

Vulnerability Management

Betterworks engages with third parties for end-to-end penetration testing and vulnerability scanning.

System Monitoring

Betterworks monitors capacity with tools to ensure that system resources are adequate to allow customer access to data. System performance and capacity thresholds are configured to alert the Operations Center. Tickets are created to document and track issue resolution.

Incident Response

Betterworks' incident management policies cover incidents that may affect the security and integrity of customer data and its information assets, and outlines steps to take in the event of such an incident. Betterworks intends to ensure that the company is prepared if a security incident were to occur.

Documentation is in place outlining what must occur if an incident is suspected, covering both electronic and physical security incidents. Specifically, this documentation includes reporting the incident, root cause analysis, logging events in change management system, restoring any systems as necessary, taking steps to ensure similar vulnerabilities will not reappear, and reflecting and learning about the incident to suggest additional changes or improvements.

Change Management

Change management procedures help ensure that changes to Betterworks systems do not result in data becoming unavailable outside of predetermined times. Changes to the Betterworks application software and systems are tracked through a ticketing system. Prior to deployment, engineers peer review and product owners approve changes. Engineering reviewers assess changes that affect security, availability, confidentiality, and privacy of Customer Data. Product reviewers check for adherence to product specifications, consistency, and usability. The review process also includes automatic and manual peer QA testing, performance and scalability, and test deployments.

Additionally, IT management monitors changes monthly, parallel with the sprint cycle, to validate they were peer reviewed prior to implementation into production. If changes were implemented without peer review, the contents of the change are reviewed and reverted from production if needed.

Backups and Disaster Recovery

In the event of a system failure, for any reason including natural disasters, Betterworks has implemented a Backup and Recovery policy to limit customer impact. A backup plan is in place that includes full backups, at least daily. Additionally, management maintains a formal disaster recovery plan, which is updated and tested annually.

Data Management

Security standards and procedures including a data classification policy promote secure transmission and storage of confidential customer data.

At any time during the then-current term of the applicable order form between Betterworks and its Customer, Betterworks will provide Customer with access to the Customer Data, in the then-current standard export format or another industry-standard format mutually agreed by the parties. At expiration, Betterworks shall delete Customer Data within 30 (thirty) days of termination.

Privacy

Betterworks maintains a Privacy Notice on the publicly available website including privacy practices related to notice, choice and consent, collection, use, retention, disposal, access, and third-party disclosure. Additionally, management maintains an internal Privacy Policy available for internal employees related to the collection, handling, retention, and disposal of customer information.

The Legal team performs a semiannual privacy review over the following:

- Publicly facing Privacy Notice
- Internal Privacy Policy
- Personal Information collection practices
- Terms and Conditions document
- List of third-party providers with whom data is shared, including the date of disclosure
- Validation that deactivated customer data has been removed or anonymized from the application

Within the platform, end users have the ability to view their personal information via the Profile feature. Input validation checks are built into the Betterworks Platform to prevent inaccurate data form being input. Company administrator users have the ability to update user information. Alternatively, requests can be emailed to support@betterworks.com, including requests for access to or deletion of personal information. The Support team authenticates and processes such requests within 30 (thirty) days.

Information and Communication

To help align Betterworks business strategies and goals with operating performance, management is committed to maintaining effective communication with personnel. Management across functional areas participates in weekly meetings to discuss the status of service delivery or other matters of interest and concern.

Internal Communications

Management presents key corporate and department goals, summarized financial results, and critical operational performance to Betterworks employees during frequent, company-wide meetings. Information on Betterworks policies, procedures, and security concerns are communicated in trainings and company-wide meetings. In addition, new employees are briefed on Betterworks security policy during employee orientation. Each employee signs a security acknowledgement form and a confidentiality agreement. This interaction enables personnel to identify and readily communicate issues or suggestions to management for consideration and resolution.

External Communications

Betterworks provides information to its customers through the Terms and Conditions associated with each applicable customer order form. The Terms and Conditions also reference the Privacy Notice and practices in place. These documents include delineation of the boundaries of the system and services, purpose of the services, customer roles and responsibilities related to data security, confidentiality, availability, and privacy. The always-current Privacy Notice is available on the public Betterworks website at https://www.betterworks.com/privacy-notice/. Alternatively, see *Appendix A* for the then-current Betterworks Privacy Notice as of the effective date of this report.

Monitoring

Betterworks uses tools to monitor system resources, performance, and access control. The Engineering team receives notifications when application errors occur or system resources are strained. Betterworks policies require sufficient financial and personnel resources allocated to monitoring production systems.

Additionally, external third parties perform penetration testing, a risk assessment, and an internal audit over Betterworks' security controls on an annual basis. Significant findings are tracked and monitored to resolution.

The Betterworks Security Council annually monitors and reviews subservice organizations to ensure they continue to deliver required level of security and services. Similarly, the Security Council monitors and reviews internal policies to ensure compliance. The policies require sufficient financial and personnel resources to ensure Betterworks can continue to validate its adherence to policies and procedures.

Complementary User Entity Controls

Betterworks' control environment was designed under the assumption that certain controls would be implemented by user organizations, the application of which is necessary to meet certain trust services criteria identified in this report. This section highlights those internal control responsibilities Betterworks believes should be present at each customer and has considered in developing its controls reported on herein. Betterworks customers should evaluate their own control environment to assess if the following controls are implemented and operating effectively. These complementary user entity controls do not represent a comprehensive list of controls that should be employed by Betterworks customers, but are rather a summary of controls necessary to meet the stated trust services criteria presented in this report. These controls include the following:

- Customers utilizing single sign-on for authentication are responsible for ensuring appropriate configuration (Common Criteria 6.1).
- Customers are responsible for ensuring granting and removing access to Betterworks in accordance with end users' authorization, including Betterworks customer support personnel (Common Criteria 6.1, 6.2, 6.3).
- Customers are responsible for ensuring communications of personal information is performed in a secure manner through defined shared folders hosted on Box.com (Common Criteria 6.7).
- Customers are responsible for ensuring data entered or changed in Betterworks is in accordance with the provisions of contractual agreements or other applicable governing agreements (Confidentiality 1.1, Privacy 7.1).
- Customers are responsible for ensuring they obtain consent to collect personal information from the users whose data is shared with Betterworks (Privacy 3.2).

Complementary Subservice Organization Controls

Betterworks contracts with Amazon Web Services and Heroku to host front-end production systems used to deliver, support, and protect the Goal Setting & Continuous Performance Management Platform environment, and Box.com for securely transmitting and storing customer-specific documents. Controls managed by these third-party subservice providers are not included in the scope of this report. Expected subservice provider controls that have an effect on specific criteria are included below.

Criteria	Controls expected to be in place at AWS and Box	Controls expected to be in place at Heroku
CC6.1 – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Access to the in-scope systems requires users to authenticate using a valid unique user ID and password before being granted access. Users are authenticated prior to accessing system components. Encryption keys are logically secured.	Access to the in-scope systems requires users to authenticate using a valid unique user ID and password before being granted access. Users are authenticated prior to accessing system components.
CC6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	User accounts are approved by appropriate individuals prior to being provisioned.	User accounts are approved by appropriate individuals prior to being provisioned.

Criteria	Controls expected to be in place at AWS and Box	Controls expected to be in place at Heroku
CC6.3 – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	User accounts are removed when access is no longer needed or users are terminated. User accounts are reviewed on a regular basis by appropriate personnel.	User accounts are removed when access is no longer needed or users are terminated. User accounts are reviewed on a regular basis by appropriate personnel.
CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Physical access to computer facilities housing the production systems is restricted to authorized users.	Not applicable.
CC6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Discontinued physical assets are physically destroyed prior to leaving facilities.	Not applicable.
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network security mechanisms are in place to restrict external access to the production environment. Encrypted communication is required for connections to the production system.	Network security mechanisms are in place to restrict external access to the production environment. Encrypted communication is required for connections to the production system.

Criteria	Controls expected to be in place at AWS and Box	Controls expected to be in place at Heroku
CC6.7 – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Customer data is protected during transmission, movement, and removal.	Customer data is protected during transmission, movement, and removal.
CC6.8 – The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Anti-virus or anti-malware applications are installed to detect or prevent unauthorized or malicious software.	Anti-virus or anti-malware applications are installed to detect or prevent unauthorized or malicious software.
CC7.2 – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Vulnerabilities are logged, investigated, and tracked to resolution.	Vulnerabilities are logged, investigated, and tracked to resolution.
CC7.3 – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Vulnerabilities, incidents, and security events are evaluated and tracked to resolution.	Vulnerabilities, incidents, and security events are evaluated and tracked to resolution.
CC7.4 – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Incidents are logged, assigned severity ratings, and tracked to resolution.	Incidents are logged, assigned severity ratings, and tracked to resolution.

Criteria	Controls expected to be in place at AWS and Box	Controls expected to be in place at Heroku
CC8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	System changes are documented, tested, and approved prior to migration to production.	System changes are documented, tested, and approved prior to migration to production.
A1.1 – The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Monitoring processes alert appropriate personnel when capacity thresholds are exceeded.	Monitoring processes alert appropriate personnel when capacity thresholds are exceeded.
A1.2 – The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Environmental protections, including backup controls, are implemented in the production environment.	Environmental protections, including backup controls, are implemented in the production environment.
A1.3 – The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Backups are tested.	Backups are tested.
C1.1 – The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Customer data is retained upon request. Customer data is redundantly stored across locations.	Customer data is retained upon request. Customer data is redundantly stored across locations.
C1.2 – The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Customer data is deleted upon request.	Customer data is deleted upon request.