Chili Piper, Inc
Type 1 SOC 2
2018

REPORT ON CHILI PIPER, INC'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN OF ITS CONTROLS RELEVANT TO SECURITY

Pursuant to Reporting on Service Organization Controls 2 (SOC 2)
Type 1 examination performed under AT-C 105 and AT-C 205

June 30, 2018

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS AT CHILI PIPER, INC RELEVANT TO SECURITY

To Chili Piper, Inc:

We have examined the attached description titled "Description of Chili Piper, Inc's Software-as-a-Service (Scheduling Automation) System as of June 30, 2018" (the description) and the suitability of the design of controls to meet the criteria for the Security principles set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), as of June 30, 2018. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Chili Piper, Inc's ('Chili Piper' or 'the Company') controls are suitably designed, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

Chili Piper uses Google Cloud Platform for data center hosting services and Amazon S3 for backup storage ("subservice organizations"). The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organizations are suitably designed. The description presents Chili Piper's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, and suitably designed at the subservice organizations to meet certain applicable trust services criteria. The description does not include any of the controls implemented at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations.

Chili Piper has provided the attached assertion titled "Management of Chili Piper, Inc's Assertion Regarding Its Software-as-a-Service (Scheduling Automation) System as of June 30, 2018," which is based on the criteria identified in management's assertion. Chili Piper is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in Chili Piper's assertion and on the suitability of the design of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination 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, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed to meet the applicable trust services criteria as of 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 the suitability of the design of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed to meet the applicable trust services criteria. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We did not perform any procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, do not express an opinion thereon. Because of their nature and inherent limitations, controls at a service organization may not prevent, or detect and correct, all errors or omissions 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 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.

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

a. the description fairly presents the system that was designed and implemented as of June 30, 2018, and
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 as of June 30, 2018, and user entities applied the complementary user-entity controls contemplated in the design of Chili Piper's controls as of June 30, 2018 and the subservice organization applied, as of June 30, 2018, the types of controls expected to be implemented at the subservice organization and incorporated in the design of the system.

This report is intended solely for the information and use of Chili Piper; user entities of Chili Piper's Software-as-a-Service (Scheduling Automation) System as of 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.
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria.
- The applicable trust services criteria.
- 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.

A-LIGN

July 2, 2018
Tampa, Florida

SECTION 2

MANAGEMENT OF CHILI PIPER, INC'S ASSERTION REGARDING ITS SYSTEM AS OF JUNE 30, 2018

Management of Chili Piper, Inc's Assertion Regarding Its System as of June 30, 2018

July 2, 2018

We have prepared the attached description titled "Description of Chili Piper, Inc's Software-as-a-Service (Scheduling Automation) System as of 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 paragraphs 1.34-.35 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the Software-as-a-Service (Scheduling Automation) System, particularly system controls intended to meet the criteria for the Security principles set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that:

a. the description fairly presents the Software-as-a-Service (Scheduling Automation) System as of 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:

      - *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
      - *Software*. The application programs and IT systems software that supports application programs (operating systems, middleware, and utilities).
      - *People*. The personnel involved in governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
      - *Processes*. The automated and manual procedures.
      - *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) How the system captures and addresses significant events and conditions.

      (5) The process used to prepare and deliver reports and other information to user entities or other parties.

      (6) If information is provided to, or received from other parties, how such information is provided or received; the role of the other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

      (7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system.

      (8) Any applicable trust services criteria that are not addressed by a control at the service organization and the reasons therefore.

      (9) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(10) 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 user may consider important to his or her own particular needs.

b. the controls stated in description were suitably designed throughout the specified period to meet the applicable trust services criteria.

Nicolas Vandenberghe

Nicolas Vandenberghe
Co-founder
Chili Piper, Inc

SECTION 3

DESCRIPTION OF CHILI PIPER, INC'S SYSTEM AS OF JUNE 30, 2018

OVERVIEW OF OPERATIONS

Company Background

Chili Piper was founded in 2016 with the mission to build a new B2B SaaS category: Customer Tech.

Description of Services Provided

Chili Piper currently offers a suite of two products. One for sales. One for marketing. For marketing, Chili Piper has developed a product that integrates with all web forms via a JavaScript snippet or APIs. The Chili Piper form booker allows teams to provide a better customer buying experience by prompting qualified leads that submit demo requests/contact requests to book a meeting with the right sales rep immediately upon form submission. The meetings are routed in real time to the right sales rep and logged in Salesforce ensuring fair distribution and accurate distribution of meetings.

The Chili Piper sales handoff product offers an advanced way for teams to schedule meetings across their entire company from SDR to AE to CSM to Support. The Company has built Chili Piper as a connected app in Salesforce using its APIs and a simple connection to Office 365 and Google Apps to provide reps with the ability to schedule meetings in two clicks via phone and offer one click suggested time slots. The product can support any and every complex sales handoff use case from a simple round robin to advanced territory and named account assignments. Upon booking the meeting the sales reps are notified, meetings are logged in Salesforce, and reminders are queued up to increase show rates.

For Sales:

- Sales Handoff - Salesforce Integration
- Google/Office 365 Calendar Integration
- SDR -> AE Handoff Solution
- Round Robin Management
- Advanced Meeting Routing (territory, company size, etc.)
- Integrations w/ Zoom, GoToMeeting, and more
- No-Show Management

For Marketing:

- Intelligent Form Booker - Schedule Meetings from Contact Us/Request Demo Forms
- Integrates w/ Marketo, Eloqua, Hubspot, Pardot, and many more
- Match Leads to Existing Salesforce Owner
- Real-Time Lead Routing + Calendar
- Disqualify Leads who aren't a fit
- API access for customization
- Advanced reporting

Infrastructure

Primary infrastructure used to provide Chili Piper's Software-as-a-Service (Scheduling Automation) system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Containers	Kubermetes	Container orchestration
Containers	Kubernet Cluster	Automate container and dev deployment
Production Server	MongoDB	Production server database
Backup + Storage	Amazon S3	Encryption and storage via Amazon s3

Software

Primary software used to provide Chili Piper's Software-as-a-Service (Scheduling Automation) system includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Google Cloud	MacOS	Hosting for main app
Amazon AWS	MacOS	Hosting for marketing site
Dreamhost	MacOS	Hosting testing accounts
Browserstack	MacOS	Testing different browsers
DigitalOcean	MacOS	For site www.chilipiper.com
Salesforce	MacOS	Sales crm
Pandadoc	MacOS	E-signature
Paypal	MacOS	Invoices
Jira	MacOS	Engineering tasks
Google suite	MacOS	E-mail etc
Helpscout	MacOS	Support
Dropbox	MacOS	Due diligence
Figma	MacOS	Design
Nuclino	MacOS	Engineering documentation
Clearbit	MacOS	Data enrichment
Airtable	MacOS	Product planning

People

The Chili Piper staff provide support for the following areas:

- Executive team - provides overall strategic moves and insight on planning, operations, and plans as a company
- Development team - develops the app
- QA team - tests the app to make sure it works properly and report any bugs
- CSM team - to support and onboard customers
- Support team - to maintain support with customers to assure proper use of the app
- System admin - provision and deprovision apps for users across the team
- Sales team - to make money

Processes

IT policies describe physical, logical security and our security policy. These are located on the security folder in Google Drive for new employees to review and acknowledge.

Physical Security

All operations run on the Google Cloud Platform. Backups are stored on Amazon S3. OAuth tokens are also stored at S3 using native encryption. Chili Piper, Inc follows the Google Security model.

All new employees are given access to WeWork (shared office space) and all minute details are handled by WeWork including visitors, building access, etc. Access to the building is granted by a badge scan. Upon receipt of a company computer, employees are instructed to follow protocols to lock the computer after a period of 15 minutes of inactivity.

Upon termination employees must return materials that allow them to access WeWork during working hours.

Logical Access

Upon hire, a new employee must acknowledge the logical security located in the security policy. The logical security is reviewed on an annual ongoing basis and this is used to help HR grant access permissions to apps for new employees and permission access to apps for terminated employees.

Developers accessing the production network are given access via VPN for remote access by a secure system.

Each tenant is hosted in a separate MongoDB database instance. All in-transit data is encrypted with 256-bit SSL. Only the CTO and system administrator have access to databases, for technical purposes only, via two-factor authentication.

Computer Operations - Backups

Chili Piper, Inc stores backups on Amazon S3. All of the data is stored on the cloud. Nothing is stored locally. Incremental Backups must be saved for one month. Full Backups must be saved for one year. RTO shall be 4 hours. RPO shall be 24 hours. All databases must be redundant in real time using MongoDB secondary servers. In addition, backups located in a different geographic zones must be made as follows:

- Incremental: every day
- Full: every 3 days

Computer Operations - Availability

Incident response policies are in place to guide employees and customers on how to report and respond to IT incidents of each type: global, continent, and business. Incident severity is defined by high, medium, and low and the policy for internal employees is for all staff to report any incidents or suspected incidents immediately by contacting the person in charge as highlighted in the incident categorization above.

Security events, for example a virus infection, could quickly spread and cause data loss across the organization. All users must understand, and be able to identify that any unexpected or unusual behavior on the workstation could potentially be a software malfunction. If an event is detected users must:

- Note the symptoms and any error messages on screen
- Disconnect the workstation from the network if an infection is suspected (with assistance from the support team highlighted in this document from the IT department)
- Not use any removable media (for example USB memory sticks) that may also have been infected

All suspected security events should be reported immediately to the IT support team listed above. If the incident is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported to the HR Support team above.

Change Control

Chili Piper maintains a documented development life cycle using Jira as the records for the engineering and product team. QA and testing are documented and maintained within Jira upon completed tasks that will be pushed to production. Chili Piper, Inc has a testing and production environment to maintain efficient process for the development team.

Data Communications

Firewall systems are in place to filter correct inbound traffic. Admin access is restricted to the dev team and front-end web developer. Chili Piper, Inc conducts a penetration test annually. The entity's penetration test is conducted to ensure they meet security standards of their app. Penetration testing includes:

- Determining how well the Chili Piper systems under test can tolerate real-world style attack patterns
- Determining the level of sophistication an attacker needs to successfully compromise a Chili Piper system
- Identifying what additional countermeasures could mitigate the threats to affected Chili Piper systems

Backbone Security reviewed the security of Chili Piper's in-scope infrastructure and has determined that a low risk of compromise exists from external attackers.

Authorized employees may access the server via VPN technology.

Data

Incident reports are documented in Jira. Alerts are sent out to admins and users via Intercom of any known issues to keep transparent communication with customers. Customer data is stored in accordance with the data protection policy. Chili Piper, Inc uses Amazon S3 for storage and encryption. Backups occur on regular intervals and the entity is GDPR compliant with customer data in Europe as seen in section 5 of the terms and conditions.

Boundaries of the System

The scope of this report includes the Software-as-a-Service (Scheduling Automation) system performed in the New York, New York facilities.

This report does not include the data center hosting services provided by Google or the backup storage services provided by Amazon S3.

Significant Events and Conditions

Chili Piper has a documented procedure for incident reporting in place to manage special events and conditions. Please see the incident management policy for customers and employees.

Preparation and Delivery of Reports and Data

Chili Piper, Inc utilizes the services and procedures described above to capture, prepare, and deliver reports and other information (described in the data section above) to user entities and other parties.

Subservice Organizations

The data center hosting services provided by Google are monitored by management; however, they have not been included in the scope of this review. The following criteria and controls are expected to be implemented by Google.

Subservice Organization Controls - Google		
Principle	**Criteria**	**Applicable Controls**
Security	CC5.5	Annual data center security reviews are performed and results are reviewed by executive management
Security	CC5.5	Physical security measures in place include:

Subservice Organization Controls - Google		
Principle	**Criteria**	**Applicable Controls**
		• Existence of security guards, access badges, and video cameras to secure the data centers • Data center entrances have a perimeter security system consisting of badge readers or biometric access system
Security	CC5.5	User access lists to data center server areas are reviewed on a quarterly basis and inappropriate access is removed in a timely manner
Security	CC5.5	Equipment is not permitted to leave the data center without being subject to Google's sanitization process
Security	CC5.5	Access to production machines must be approved by group administrators

The backup storage services provided by Amazon S3 are monitored by management; however, they have not been included in the scope of this review. The following criteria and controls are expected to be implemented by Amazon.

Subservice Organization Controls - Google		
Principle	**Criteria**	**Applicable Controls**
Security	CC5.5	Physical access to data centers is approved by an authorized individual
Security	CC5.5	Physical access is revoked within 24 hours of the employee or vendor record being deactivated
Security	CC5.5	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel
Security	CC5.5	Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited to 30 days by legal or contractual obligations
Security	CC5.5	Physical access points to server locations are managed by electronic access control devices
Security	CC5.5	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents

Criteria Not Applicable to the System

All Common criteria was applicable to the Chili Piper, Inc Software-as-a-Service (Scheduling Automation) system.

Significant Changes in the Last 12 Months

No significant changes have occurred to the services provided to user entities or in the 12 months preceding the end of the review period.

CONTROL ENVIRONMENT

Integrity and Ethical Values

Chili Piper has a formally documented control environment policy and code of conduct for new employees to review and acknowledge. Background checks are done prior to a new employee coming on board via Checkr. Policies are required to be reviewed and acknowledged by new employees. All of this documentation can be found in the HR Google Drive.

Commitment to Competence

Management considers competence to be what is required to get the job done correctly and on time for all positions. Training is provided to all departments to increase competence and proper measures are set in place to improve competence over time.

Management's Philosophy and Operating Style

Management meets in daily scrums with all departments. Management holds weekly company meetings to cover product and sales to make sure the team is on the same page of company news. Management regularly reviews internal policies and lets employees determine their work schedule during the remote work environment provided at Chili Piper.

Organizational Structure and Assignment of Authority and Responsibility

Chili Piper, Inc's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Chili Piper, Inc'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 appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring 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 charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.

Human Resources Policies and Practices

Chili Piper, Inc's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Chili Piper, Inc's human resources 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:

- New employees are required to sign acknowledgement forms for the employee handbook
- Evaluations for each employee are performed on a weekly basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

RISK ASSESSMENT

Chili Piper's risk assessment process identifies and manages risks to identify significant risks inherent in products or services as they oversee their areas of responsibility. Chili Piper implements appropriate measures to monitor and manage the risks. This process has identified risks and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk (changes in the environment, staff, or management personnel)
- Strategic risk (new technologies, changing business models, and shifts within the industry)
- Compliance (to make sure the entity is legally and data compliant with the customers)

Chili Piper, Inc's executive team and development teams are responsible for identifying organizational risk and strategic risk assessments at an ongoing basis.

TRUST SERVICES PRINCIPLES AND CRITERIA

In-Scope Trust Services Principles

Common Criteria (*to all Security Principles)*
The security principle refers to the protection of the system resources through logical and physical access control measures in order to enable the entity to meet its commitments and system requirements related to security, availability, processing integrity, confidentiality, and privacy. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Chili Piper, Inc's Software-as-a-Service (Scheduling Automation) system; as well as the nature of the components of the system result in risks that the criteria will not be met. Chili Piper, Inc addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Chili Piper, Inc's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Control Activities Specified by the Service Organization

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC1.0	**Common Criteria Related to Organization and Management**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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.	A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority. Reporting relationships and organizational structures are reviewed annually by management. Roles and responsibilities are defined in written job descriptions and communicated to personnel. Management reviews job descriptions annually and makes updates, if necessary.
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.	A documented organizational chart is in place to assign responsibility and delegate lines of authority to personnel. Roles and responsibilities are defined in written job descriptions and communicated to personnel. Management reviews job descriptions as needed and makes updates, if necessary.
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.	Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process. The experience and training of candidates for employment of transfer are evaluated before they assess the responsibilities of their position. Employees are required to read and acknowledge information security policies and complete information security training upon hire.
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.	An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures. Personnel are required to sign and accept the code of conduct upon hire.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC2.0	**Common Criteria Related to Communications**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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.	System descriptions are communicated to authorized external users via entity website that delineate the boundaries of the system and describe relevant system components. A description of the system delineating the boundaries of the system is posted on a secure network drive and is available to personnel. A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority. Reporting relationships and organizational structures are reviewed annually by management. Roles and responsibilities are defined in written job descriptions and communicated to personnel.
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.	Security commitments are communicated to external users via the entity's website. Policy and procedure are documented for significant processes are available on the entity's intranet. Employees are required to read and acknowledge information security policies and complete information security training upon hire. Personnel are required to sign and accept the code of conduct upon hire.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	Policy and procedure are documented for significant processes are available on the entity's intranet. Roles and responsibilities are defined in written job descriptions and communicated to personnel. Management reviews job descriptions as needed and makes updates, if necessary.
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.	Processes are monitored through service level management procedures to help ensure compliance with service level commitments and agreements. Employees are required to read and acknowledge information security policies and complete information security training upon hire.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC2.0	**Common Criteria Related to Communications**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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.	The organization's security policies and code of conduct are communicated to employees in the employee handbook. Documented incident response policies and procedures are in place to guide personnel in the event of an incident.
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.	Application changes are authorized, tested, and approved by management prior to implementation. Application changes are communicated to both internal and external users.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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.	A master list of the entity's system components is maintained, accounting for additions and removals, for management's use. Documented policies and procedures are in place to guide personnel when performing the risk assessment process. A formal risk assessment is performed on an annual basis to identify threats that could impair systems security commitments and requirements. Identified risks are rated using a risk evaluation process and rating are reviewed by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process.
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.	Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances. External vulnerability scans and penetration tests are performed on an annual basis and remedial actions are taken. Business continuity and disaster recovery plans are developed and updated on an annual basis.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC4.0	**Common Criteria Related to Monitoring Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Control self-assessments that include, but are not limited to, logical access reviews, and backup restoration tests are performed on an annual basis. Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. The monitoring software is configured to alert appropriate personnel when thresholds have been exceeded. Penetration tests are performed on an annual basis and remedial actions are taken.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Documented policies and procedures are in place regarding access, and security monitoring. Logical access to systems is granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process.
	Network	
		Network user access is restricted via role based security privileges defined within the access control system. Network administrative access is restricted to user accounts accessible by the following personnel: • Software Developer • Quality Assurance & Customer Success Network users are authenticated via individually-assigned user accounts and passwords. Networks are configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity Network account lockout procedures are in place.
	Database	
		Database user access is restricted via role based security privileges defined within the access control system. Database administrative access is restricted to user accounts accessible by the following personnel: • Software Developer • Quality Assurance & Customer Success Database users are authenticated via individually-assigned user accounts and passwords.
	Application	
		Application user access is restricted via role based security privileges defined within the access control system.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Application administrative access is restricted to user accounts accessible by the following personnel: • Software Developer • Quality Assurance & Customer Success Application users are authenticated via individually-assigned user accounts and passwords. The application is configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity Application account lockout procedures are in place. Application access reviews are completed by management on an annual basis.
	Remote Access	
		VPN user access is restricted via role based security privileges defined within the access control system. The ability to administer VPN access is restricted to user accounts accessible by appropriate personnel. VPN users are authenticated username and password to being granted remote access to the system. Privileged access to sensitive resources is restricted to defined user roles.
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.	Documented policies and procedures are in place regarding access and security monitoring. Logical access to systems is granted to an employee as a component of the hiring process. Logical and physical access to systems is revoked as a component of the termination process. Account sharing is prohibited unless a variance from policy is granted by management.
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.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Logical and physical access to systems is granted to an employee as a component of the hiring process. Control self-assessments that include logical access reviews are performed on an annual basis.
	Network	
		Network user access is restricted via role based security privileges defined within the access control system. Network administrative access is restricted to user accounts accessible by the following personnel: • Quality Assurance & Customer Success Network users are authenticated via individually-assigned user accounts and passwords. Networks are configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity Network account lockout procedures are in place.
	Database	
		Database user access is restricted via role based security privileges defined within the access control system. Database administrative access is restricted to user accounts accessible by the following personnel: • Software Developer • Quality Assurance & Customer Success Database users are authenticated via individually-assigned user accounts and passwords.
	Application	
		Application user access is restricted via role based security privileges defined within the access control system. Application administrative access is restricted to user accounts accessible by the following personnel: • Software Developer • Quality Assurance & Customer Success

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Application users are authenticated via individually-assigned user accounts and passwords. The application is configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity Application account lockout procedures are in place. Application access reviews are completed by management on an annual basis.
	Remote Access	
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.	VPN user access is restricted via role based security privileges defined within the access control system. The ability to administer VPN access is restricted to user accounts accessible by appropriate personnel. VPN users are authenticated username and password to being granted remote access to the system. Users can only access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system. Documented policies and procedures are in place regarding systems authentication, access, and security monitoring. Logical and physical access to systems is granted to an employee as a component of the hiring process. Logical and physical access to systems is revoked as a component of the termination process. Control self-assessments that include logical access reviews are performed on an annual basis.
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.	This criterion is managed by the subservice provider. Please refer to Section 3 for the controls managed by the subservice provider.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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.	A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority. Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.
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.	SSL technologies are used for defined points of connectivity. Documented procedures exist to secure the network infrastructure. The workstations are password protected and automatically logoff if the system is unattended.
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.	The ability to migrate changes into the production environment is restricted to authorized and appropriate users. A file integrity monitor is in place to ensure only authorized changes are deployed into the production environment. The file integrity monitoring application is configured to notify appropriate personnel via e-mail alert when a change to the production application code files is detected. External vulnerability scans and penetration tests are performed on an annual and remedial actions are taken.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC6.0	**Common Criteria Related to System Operations**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. The monitoring software is configured to alert appropriate personnel when thresholds have been exceeded. Documented incident response policies and procedures are in place to guide personnel in the event of an incident. Data backup and restore procedures are in place to guide personnel in performing backup activities. An automated backup system is utilized to perform scheduled system backups. Full backups of certain application and database components are performed every three days and incremental backups are performed on a daily basis. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.
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.	Documented incident response policies and procedures are in place to guide personnel in the event of an incident. A ticket tracking application is utilized to track and respond to incidents. Resolution of incidents is communicated to users within the corresponding ticket. Change management requests are opened for events that require permanent fixes. Entity policies include progressive discipline up to and including termination for employee misconduct.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC7.0	**Common Criteria Related to Change Management**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Documented change control policies and procedures are in place to guide personnel in the handling system changes. Application changes are authorized, tested, and approved by management prior to implementation. Access to the following is restricted to appropriate personnel: • Make Changes In The Development Environment • Deploy Changes Into The Production Environment • Approve System Changes • Approve Infrastructure Changes • Program Source Code
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.	Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances. A formal risk assessment is performed on an annual basis to identify threats that could impair systems security commitments and requirements. Identified risks are rated using a risk evaluation process and rating are reviewed by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process.
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.	Documented escalation procedures for reporting security incidents are in place to guide users in identifying and reporting failures, incidents, concerns, and other complaints. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.
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.	Documented change control policies and procedures are in place to guide personnel in the handling system changes. Application change requests are documented and tracked in a ticketing system. Application changes are tested prior to implementation. Types of testing performed depend on the nature of the change.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC7.0	**Common Criteria Related to Change Management**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Application changes are approved by management prior to implementation. Application changes are communicated to both internal and external users. Development and test environments are physically and logically separated from the production environment. Access to implement changes in the production environment is restricted to authorized IT personnel. File integrity monitoring software is utilized to help detect unauthorized changes within the production environment. Prior code is held in the repository for rollback capability in the event that a system change does not function as designed. The change management process has defined the following roles and assignments: • Authorization of change requests-owner or business unit manager • Development-application design and support department • Testing-quality assurance department • Implementation software change management group

MONITORING

Management monitors controls on an ongoing basis to conduct QA efforts to ensure correct actions are taken. Chili Piper, Inc uses a tool for system security monitoring that has file integrity monitoring also, called OSSEC. This tool monitors and documents results at an ongoing result and risks identified receive high rates and are handled as high priority by management. Adherence to employee policies and activity are also monitored at an ongoing basis to ensure employee and company compliance with HR standards documented by management.

On-Going Monitoring

Chili Piper, Inc's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Chili Piper, Inc's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Chili Piper, Inc's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

INFORMATION AND COMMUNICATION SYSTEMS

Chili Piper, Inc uses Slack and Gmail for internal communication and Zoom for internal and external meetings with the employees, customers, and prospects. Chili Piper, Inc holds weekly sales and product calls and have daily scrum meetings for all departments.

Specific information systems used to support Chili Piper, Inc's Software-as-a-Service (Scheduling Automation) system are described in the Description of Services section above.

COMPLEMENTARY USER ENTITY CONTROLS

Chili Piper's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Principles related to Chili Piper's services to be solely achieved by Chili Piper control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Chili Piper.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Principles described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Chili Piper, Inc.
2. User entities are responsible for notifying Chili Piper, Inc of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Chili Piper, Inc services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Chili Piper, Inc services.
6. User entities are responsible for providing Chili Piper, Inc with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Chili Piper, Inc of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN's examination of the controls of Chili Piper was limited to the Trust Services Principles and related criteria and control activities specified by the management of Chili Piper and did not encompass all aspects of Chili Piper's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the processing of the user entity's transactions;
- Understand the flow of significant transactions through the service organization;
- Determine whether the control objectives are relevant to the user entity's financial statement assertions; and
- Determine whether the service organization's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user entity's financial statements and determine whether they have been implemented.