APPENDIX F

Security & Data Privacy Certification Form

AFI Translation Services — Request for Proposals

Purpose

This certification form must be completed and submitted by all Offerors responding to the AFI Translation Services RFP. It serves to verify that the Offeror's practices, systems, and policies comply with applicable data security standards, data residency requirements, and restrictions on the use of agency data — including the prohibition on using agency-provided content for AI model training without explicit written consent.

Submission of this form constitutes a binding certification. Misrepresentation or material omission may result in disqualification, contract termination, and/or other remedies available under applicable law.

Part I — Offeror Identification

Legal Name of Offeror:	Effectiff LLC
DBA / Trade Name (if applicable):	N/A
Primary Business Address:	1212 Broadway Plaza, Suite 2100, Walnut Creek, CA 94596
DUNS / UEI Number:	KEKGUNCN2QB7
Name of Authorized Certifying Official:	Alex Cherkashin
Title:	Senior Director of Operations
Email Address:	Alex.ch@effectiff.com
Phone Number:	(929) 999-5719
Date of Submission:	05.06.2026

Part II — Security & Data Privacy Certification Checklist

For each requirement below, indicate compliance status and provide any relevant notes or explanations.

#	Requirement	Compliance Status	Notes / Explanation
A. Data Security Standards			
A1	Offeror maintains and operates under a documented Information Security Program (ISP) aligned with a recognized framework (e.g., NIST SP 800-53, ISO 27001, SOC 2 Type II).	☒ Yes ☐ No ☐ N/A	AiTranslate (AiT) has ISO 9001, ISO 17100, ISO 18587, and ISO 27001; Phrase CAT tool (Phrase) has ISO 27001, SOC 2 Type I certified, SOC 2 Type II expected in 2026;

			Interpretation Platform has SOC 2 Type II
A2	All data in transit is encrypted using TLS 1.2 or higher. All data at rest is encrypted using AES-256 or equivalent standard.	☒ Yes ☐ No ☐ N/A	
A3	Offeror conducts regular vulnerability assessments and penetration testing (at least annually) on systems used to process agency data.	☒ Yes ☐ No ☐ N/A	
A4	Offeror maintains a documented incident response plan and will notify the agency within 72 hours of any confirmed data breach or security incident involving agency data.	☒ Yes ☐ No ☐ N/A	
A5	Access to agency data is restricted to authorized personnel only, governed by role-based access controls (RBAC) and the principle of least privilege.	☒ Yes ☐ No ☐ N/A	
A6	Multi-factor authentication (MFA) is enforced for all personnel accessing systems that process or store agency-provided content.	☒ Yes ☐ No ☐ N/A	
A7	Offeror maintains audit logs of all access to and handling of agency data, retained for a minimum of 12 months.	☒ Yes ☐ No ☐ N/A	Yes, for AiT; Audit logs are available to Phrase engineers and can be provided upon request. Login history (including IP address, country and user agent identification) is available to each user and accessible via the UI. Interpretation platform maintains a detailed audit trail recording user actions regarding rates, permissions, and system logins. However, the specific activity log data (interpreters, logs) is only stored for two months within the portal.
B. Data Residency & Sovereignty			
B1	All agency-provided data will be stored, processed, and transmitted exclusively within the United States, unless an alternative jurisdiction has been expressly approved in writing by the agency.	☒ Yes ☐ No ☐ N/A	
B2	Offeror will not transfer, replicate, or back up agency data to servers, cloud regions, or subcontractors located outside the approved jurisdiction without prior written agency authorization.	☒ Yes ☐ No ☐ N/A	
B3	Offeror can identify and document the specific data centers and/or cloud regions used to process and store agency content upon request.	☒ Yes ☐ No ☐ N/A	Virginia Data Center; North Virginia (AWS)
B4	Subcontractors and third-party vendors used in the delivery of translation services are bound by data residency obligations no less restrictive than those in this certification.	☒ Yes ☐ No ☐ N/A	

C. AI & Machine Translation — Prohibition on Unauthorized Training			
C1	Offeror will NOT use agency-provided documents, content, translations, glossaries, terminology databases, or any derivative thereof to train, fine-tune, update, or improve any AI or machine learning model without the agency's explicit prior written consent.	☒ Yes ☐ No ☐ N/A	
C2	If machine translation (MT) engines or large language models (LLMs) are used in the workflow, Offeror confirms that agency data is processed in a data-isolated environment and is not retained by the MT/LLM provider beyond the scope of the individual translation task.	☒ Yes ☐ No ☐ N/A	
C3	Offeror discloses the use of any third-party MT engines, AI translation tools, or LLM APIs (including the provider name and model) in the space provided on this form.	☒ Yes ☐ No ☐ N/A	OpenAI, Gemini, Mistral, Anthropic, Cohere; 122 general purpose Neural Machine Translation (NMT) engines
C4	Offeror has contractual agreements with any MT/LLM third-party providers explicitly prohibiting those providers from using agency data for model training, product improvement, or any purpose beyond task execution.	☒ Yes ☐ No ☐ N/A	
C5	Offeror will promptly notify the agency if any MT/LLM provider changes its data usage terms in a manner that could affect compliance with this certification.	☒ Yes ☐ No ☐ N/A	
C6	Upon contract expiration or termination, Offeror and all sub-processors will securely delete or return all agency-provided data within 30 days and provide written certification of deletion.	☒ Yes ☐ No ☐ N/A	
D. Personnel & Subcontractor Obligations			
D1	All personnel (including subcontractors) with access to agency data are bound by written confidentiality agreements and have received data privacy and security training within the past 12 months.	☒ Yes ☐ No ☐ N/A	
D2	Offeror has conducted background checks on all personnel who will have access to sensitive or controlled agency content, consistent with applicable laws and regulations.	☒ Yes ☐ No ☐ N/A	
D3	Offeror will not reassign primary translation personnel to tasks involving agency data without prior notification to the agency's Contracting Officer's Representative (COR).	☒ Yes ☐ No ☐ N/A	
E. Compliance, Certifications & Regulatory Alignment			
E1	Offeror is compliant with all applicable federal and state data privacy laws, including but not limited to FISMA, Privacy Act of 1974, and any agency-specific data handling requirements communicated in the RFP.	☒ Yes ☐ No ☐ N/A	
E2	If handling any Controlled Unclassified Information (CUI), Offeror is or will be compliant with NIST SP 800-171 and any applicable CMMC level requirements.	☒ Yes ☐ No ☐ N/A	
E3	Offeror holds or will obtain the following third-party security certifications (check all that apply): SOC 2 Type	☒ Yes ☐ No ☐ N/A	AiTranslate (AiT) has ISO 9001, ISO 17100,

	II / ISO 27001 / FedRAMP Authorization / Other (describe in notes).		ISO 18587, and ISO 27001; Phrase CAT tool (Phrase) has ISO 27001, SOC 2 Type I certified, SOC 2 Type II expected in 2026; Interpretation Platform has SOC 2 Type II
E4	Offeror will provide the agency with updated copies of relevant compliance certifications or audit reports upon request and upon renewal/expiration.	☒ Yes ☐ No ☐ N/A	

Part III — Machine Translation & AI Tool Disclosure

Offerors using any AI-assisted translation tools, machine translation engines, or large language model APIs must complete this section. If no AI or MT tools are used, indicate below and skip to Part IV.

☐ No AI or machine translation tools are used in our workflow. All translation is performed by human translators only.

Tool / Platform Name	Provider / Vendor	Role in Workflow	Data Retained by Provider?
AiTranslate	Effectiff LLC	For MT	yes
CAT tool	Phrase Solutions	Environment for localization by human supported by AI	yes
Interpretation Platform	Boostlingo LLC	For OPI and VRI	Yes, for billing only. No call recordings.

Attach copies of relevant data processing agreements (DPAs) or terms with each MT/AI provider as a sub-exhibit to this Appendix.

Please see here for Boostlingo https://boostlingo.com/customer-terms-of-service/
See here for Phrase https://phrase.com/legal/

Part IV — Exceptions & Deviations

If the Offeror cannot fully comply with any requirement listed in Part II, identify each item by number, state the nature of the limitation, and propose an equivalent alternative safeguard below. The agency reserves the right to determine whether any proposed alternative is acceptable.

Item #	Nature of Non-Compliance or Limitation	Proposed Alternative Safeguard	Estimated Compliance Date

Part V — Certification & Authorized Signature

Certification Statement

I, the undersigned authorized representative of the Offeror, hereby certify that:

- The information provided in this certification form is true, accurate, and complete to the best of my knowledge.
- The Offeror has implemented, or commits to implementing prior to contract award, all applicable security and data privacy controls described herein.
- Agency-provided data will not be used to train, fine-tune, or improve any AI or machine learning model without prior explicit written consent from the agency.
- The Offeror understands that knowingly providing false information may result in disqualification, contract termination, suspension or debarment, and/or referral for legal action.

		05.06.2026
Signature of Authorized Official		*Date*
Alex Cherkashin		Senior Director of Operations
Printed Name		*Title*

Effectiff LLC

Organization Name

Submission Instructions

This completed and signed form, along with any required attachments (DPAs, compliance certifications, sub-exhibit disclosures), must be included as Appendix F in the Offeror's proposal submission. Electronic signatures are acceptable. Unsigned or incomplete forms may result in disqualification.

CERTIFICATE

No. 42018932

LL-C Certification

This is to certify that the Information Security Management System of the company

Phrase a.s.

Václavské náměstí 2132/47
110 00 Praha 1, Nové Město
Czech Republic

The place of supply of services:
Phrase GmbH, ABC-Straße 4, 203 54, Hamburg, Germany

has been assessed and found to be in compliance with the Standard

ISO/IEC 27001:2022

applicable to

Development, maintenance and operation of Phrase Localization Platform:
- Phrase native client applications
- Phrase web applications, services and APIs
- Other related applications

Statement of Applicability (SoA): 14.9.2024

The certificate has been issued under No. **42018932** for the registration period from 31 October 2025 to 30 October 2028.
The first certificate date of issue is 15 October 2014.

Approved by

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT

S 3137

validity code: **0CF6DDE8-C09**
Check the validity of this certificate using this code at **www.ll-c.info**

Texas Risk and Authorization Management Program Certification

The information below is provided as a companion to the TX-RAMP Certification.

Cloud Service Name

Boostlingo LLC: Boostlingo On-Demand

Cloud Service Provider URL

www.boostlingo.com

Cloud Service Description (200 words or less)

From scheduling on-site, remote, and on-demand interpreters to event interpreting, AI-powered captioning, and translation services, Boostlingo provides a complete solution. Boostlingo On-Demand allows customers to manage and deliver interpretation services through phone and video. Boostlingo On-Demand Platform focuses on phone and video interpreting delivery and management. Customers can add staff interpreters or access the Boostlingo Hub for on-demand and pre-scheduled calls to 17,000 interpreters in 300+ languages. Intelligent routing, custom IVR, and call settings can be used for specialized call routing. In addition, customers can use detailed reporting for internal management and leverage built-in integrations. Boostlingo IMS automates the day-to-day coordination and management of interpretation services. The platform allows for remote and on-site services to be scheduled and managed from one place.

Certification Status

Level 2

Certificate Granted	Certification Expiration	Certificate ID
07/30/2025	07/29/2028	TX1706730

AI Translate
Security Description

AiT Overview

2.1 Access to AiT

LSI offers three ways to access AiT:

1. Customers may use a full online ordering portal (WebGate) that allows them to access all AiT services using the most popular browsers from a desktop or laptop computer anywhere. MFA is enforced for Effectiff LSI users of WebGate and configurable for Effectiff LSI clients.

2. AiT exposes a rich API, implemented as Microsoft WCF web services, that allows customers to integrate their applications with AiT.

3. For users of the eDiscovery platform Relativity, Effectiff LSI developed special Plugin applications that allows Relativity users to seamlessly access the services of AiT directly from within the Relativity environment.

2.2 High Level Architecture

Technically, AiT is a server that runs software applications built in the .NET technology.

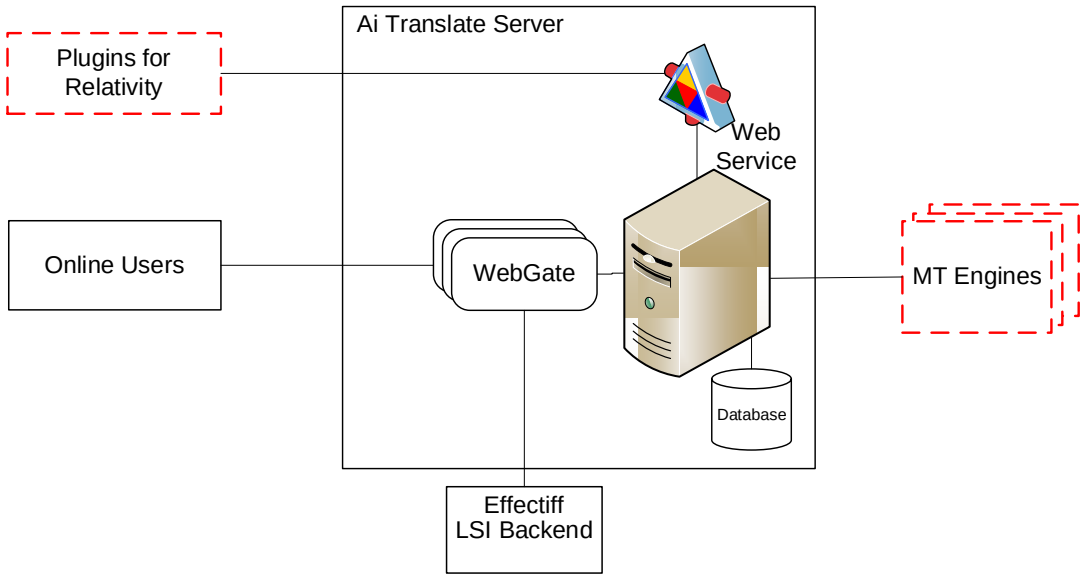


Figure 1. AiT High Level Architecture

Customers' applications and instances of Plugins for Relativity connect to AiT via API. The connection is secured by appropriate electronic security certificates.

Transport Layer

All data transfer is performed over secure 256-bit SSL channels using TLS 1.2 protocol with SHA-256 encryption additionally protected and authenticated by dedicated X-509 security certificates and IP filtering.

3.1 IP Filtering

Access to AiT API is restricted by IP Address/Range.

LSI customers accessing AiT API directly or via Relativity must register their IP addresses; otherwise, the AiT services are inaccessible.

Any changes in customers' IP address(es) must be coordinated with Effectiff LSI to prevent interruptions of the service access.

3.2 Authentication

AiT API requires Client Electronic Security Certificates to authenticate callers. AiT denies access without proper certificate.

For customers accessing AiT API directly or via Relativity, LSI may generate an X-509 client security certificate or accept such a certificate purchased by the customer from a trusted certificate authority. Any renewal or replacement of client certificates must be coordinated with Effectiff LSI prior to expiration or revocation to prevent interruptions of the service access.

AiT verifies the client certificates validity with each connection request to the service. Certificates that have been expired or revoked will result in an authentication failure.

3.3 Authorization

The provided Client Electronic Security Certificate is used to establish the identity of the caller. Only authenticated callers are authorized to execute the AiT API operations.

Data Processing and Storage

4.1 Ai Translate Job

Users may submit an order for any of AiT services using the agreed way of accessing AiT, thus creating an AiT Job.

In addition to one or more documents submitted by the customer, a new AiT Job collects or generates the relevant metadata such as billing-related information (e.g., prices, dates, etc.), the source and the target languages, the ordering user's identity and, optionally, additional Job Specifications. Also, a complete AiT Job includes the processing result, e.g., translated documents.

The AiT Job's information is considered confidential and accessible only by the ordering users and authorized Effectiff LSI personnel.

All information stored on AiT servers is encrypted.

4.2 Machine Processing

AiT performs machine translation (MT) and AI services using Effectiff LSI's proprietary engines running on the servers located within an Amazon Virtual Private Cloud (VPC).

These engines are not accessible from outside, and they have no access to external systems.

red = data in

green = data return

Figure 2. MT Data Flow

4.3 Hosting Environment Security Features

AiT servers and engines are hosted on Amazon's EC2 virtualization environment.

- Amazon Virtual Private Cloud (VPC) is a virtual network dedicated to our Amazon account. It is logically isolated from other virtual networks in the cloud and the servers inside our VPC are inaccessible from external location.
- American AiT instance runs in Amazon's US East (North Virginia) Region with a multizone database settings (for disaster recovery).
- Another AiT instance runs in Amazon's Canada Region with a multizone database settings. This AiT instance is fully independent and has no connections with the American AiT.
- The precise locations of Amazon's data centers are undisclosed.
- Amazon Certificates include SCA, CCCS, Cyber GRX, ISO 9001, ISO 27001, ISO 27017, ISO 27018, ISO 27701, PCI DSS Level 1, SOC 1, SOC 2, and SOC 3. More information can be found at: https://aws.amazon.com/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs.

LSI Premises

5.1 Human Translation, Review and Post-Editing

For human translation, review and post-editing, source and supporting materials are transferred by Effectiff LSI to the human linguistic resources (translators, editors, reviewers, etc.).

After completion of the assignment, they return the created target materials to Effectiff LSI and then destroys all the received and created materials as specified by the customers and requested by Effectiff LSI.

For the information exchange with human linguistic resources, Effectiff LSI uses secure tools such as Hightail (see 5.3.5), unless otherwise specified by the customers (for example, for special projects Effectiff LSI may set up a system that requires translators to work remotely without the ability to save any materials locally).

Effectiff LSI uses the Plunet Business Manager software application (see 5.3.6) for project management, and external human linguistic resources may have access to it unless otherwise specified by the customers.

In any case, all human resources of Effectiff LSI have NDAs in place. In addition, a customer project owner may request everyone involved in that project to sign a specific NDA provided by that customer.

5.2 Data Retention Policies

Effectiff LSI retains and destroys source and target materials as specified by the client in their Mutual Agreement. By default, the retention period is seven years.

Upon a customer's request, AiT might be configured to automatically remove the source and target materials of Machine Translation Jobs upon the delivery of the translation results. In this case, these files are stored in AiT only for the time of machine translation. This remains true even in case of an error.

For other AiT services, the system might be configured to automatically remove the source and target materials after Effectiff LSI produces the corresponding Invoices.

5.3 LSI Office Security Features

Effectiff LSI Premises are located in Boston, MA.

Effectiff LSI maintains certifications to ISO 9001, ISO 17100, ISO 18587, and ISO 27001.

5.3.1 Physical Security

- Access to the office building is monitored 24x7x365 by a security guard.
- Guests to the office building must register with the building's security guard.
- Access to the building elevators is protected 24x7x365; it requires a swipe keycard to open.
- Access to LSI's office suite is protected 24x7x365; it requires a swipe keycard to open.
- Guests to the office suite must check in at the receptionist's desk; then, they are escorted.
- Access to areas with enhanced security requirements (server room, storage rooms and cabinets) is permission-based on roles (IT and Executive committee staff).

5.3.2 Internal Data Center

- UPS power supply to the internal data center can last up to 30 minutes.
- Diverse telecom feeds.
- Fire suppression system.
- Dedicated HVAC controlling temperature and humidity.
- Disaster recovery SaaS hosted by iLand Virginia Data Center.

5.3.3 Data Security

- Data is encrypted at rest
- Continuous replication of work drives (5-minute SLA) for DR.
- Windows snapshots of work drives 4 - 6 times daily.
- Dell Unity Sans snap shots are taken daily.
- Essential servers are replicated offsite at a data center in Virginia (SSAE 16 Type 2 certified; more information about its security can be found at: http://www.iland.com/services/locations/iland-cloud-data-center-reston-virginia/).
- Backups of client data are made according to their daily schedule using the disk to cloud method. Both internal and cloud storage are encrypted.
- Client data is stored for 7 years; Sans snapshots – for less than a week; DR replication – 30 days; Windows snapshots – about two weeks (64 snapshots).

5.3.4 Data Disposition

- As per Effectiff LSI's standard record retention procedure, data is retained for at least seven years and then erased from servers, or as per specific client requirement.
- Hard drives of equipment that stores information and is slated for disposal or reuse are removed or purged/erased (either by the Manager of Information Systems on the premises, or by a third-party vendor with issuance of a certificate).
- The Manager of Information Systems maintains a database of all equipment, including items that have been taken out of service. No hard drives containing client data are sold or donated to charity.
- Data destruction disks are used to wipe clean media before disposal.
- The disposed hard drives are DOD wiped and discarded or destroyed by third party.
- The used tapes are manually destroyed.
- The Manager of Information Systems maintains records of disposed equipment.

5.3.5 Hightail security features

LSI uses Hightail for the secure information exchange with human linguistic resources.

- Enforcement of the highest level of security through setting password policies for receipt or accessing of files, expiration setting for files, as well as allowing and disallowing users.
- Hightail data centers maintain SSAE16, SOC1, and SOC2 certifications.
- Data at rest is encrypted using AES 256-bit encryption.
- All data in transit is encrypted using 128-bit SSL encryption with class 3 certificates.
- PCI and TRUSTe compliant.

5.3.6 Plunet security features

Plunet is a translation management web application that Effectiff LSI uses as its main Translation Project Management tool.

- The application is hosted in our Secured Effectiff LSI Datacenter.
- We only use HTTPS for our Plunet system, so the data is protected in transit.
- A web application penetration test is executed for each Plunet release by an external security company.
- In addition to the penetration test, a partner company of Plunet tests different aspects of the application. The test specifications are based on the OSSTMM (www.osstmm.org) methodology and the ISO/IEC 27002 standard.
- Any user input is automatically filtered and validated. The system does not accept any code, scripts, HTML or strings containing SQL syntax which reduces the risk of code injection and cross site scripting.
- An integrated session management layer ensures that only one active session is active per user login. Duplicate sessions are invalidated automatically. Furthermore, an inactive session is invalidated after a configurable timeout.
- The passwords of the application are encrypted via a unique AES-256 keystore. The private key of the keystore is then used to create a hash from each password. All passwords within the Plunet configuration file are only saved in encrypted form.
- Plunet BusinessManager has an integrated rights management system. Users can only see features and data according to their role, user profile and their access rights.

5.3.7 Effectiff LSI Personnel

- All employees, contractors and third parties are required to sign confidentiality agreements.
- All new hires have to pass background verification checks. Contractors may have to pass background checks, if the specification for a job that a contractor will work on requires it.

External Audits

Annually, Effectiff LSI's systems undergo external audits by an independent third-party auditor as required to maintain certification to ISO 9001, ISO 17100, ISO 18587 and ISO 27001.

AiT security is regularly tested (penetration/vulnerability testing) by an external Security Company. The latest Letter of Attestation was received in August 2024.

Effectiff LSI's company network is regularly tested (penetration/vulnerability testing) by an external Security Company. The latest Letter of Attestation was received in December 2024.

ISO 9001:2015

Quality Management System

SCOPE

Translation, Desktop Publishing & Interpreting Services

Certificate of Registration

Linguistic Systems, Inc.

260 Franklin Street, Boston, Massachusetts, 02110, United States

The organization at the address above has undergone an independent audit and, at the time, was found to have met the requirements of the Standard. This certificate entitles the holder of the certificate to use this conformity mark according to the terms and conditions of the application or according to the scheme holder. To verify the status of the certificate, please feel free to contact Orion at info@orioncan.com.

MSCB-362

Certificate ID:	OR-10311-1
Initial Certification:	Nov 13, 2015
Issue Date:	Nov 7, 2025
Expiry Date:	Nov 13, 2027
IAF Code:	["35 Other services"]

David Huebel, President
Orion Assessment Services International, Inc.
209-1201 Dundas Street East
Toronto, Ontario, M4M 1S2

ASSESSMENT SERVICES

www.orioncan.com

ISO 17100:2015

Translation Services

SCOPE

Provision of Translation Services

Certificate of Registration

Linguistic Systems, Inc.

260 Franklin Street, Boston, Massachusetts, 02110, United States

The organization at the address above has undergone an independent audit and, at the time, was found to have met the requirements of the Standard. This certificate entitles the holder of the certificate to use this conformity mark according to the terms and conditions of the application or according to the scheme holder. To verify the status of the certificate, please feel free to contact Orion at info@orioncan.com.

Certificate ID:	OR-10311-10
Initial Certification:	Oct 27, 2021
Issue Date:	Dec 16, 2025
Expiry Date:	Nov 04, 2027
IAF Code:	["35 Other services"]

David Huebel, President
Orion Assessment Services

ISO 18587:2017

Translation Services - Post-editing of Machine Translation Output

SCOPE

Provision of Translation Services

Certificate of Registration

Linguistic Systems, Inc.

260 Franklin Street, Boston, Massachusetts, 02110, United States

The organization at the address above has undergone an independent audit and, at the time, was found to have met the requirements of the Standard. This certificate entitles the holder of the certificate to use this conformity mark according to the terms and conditions of the application or according to the scheme holder. To verify the status of the certificate, please feel free to contact Orion at info@orioncan.com.

Certificate ID:	OR-10311-11
Initial Certification:	Oct 27, 2021
Issue Date:	Dec 16, 2025
Expiry Date:	Oct 24, 2027
IAF Code:	["35 Other services"]

David Huebel, President
Orion Assessment Services

ISO/IEC 27001:2022

Information Security Management System

SCOPE

The provision of translation and interpretation services.

Certificate of Registration

Linguistic Systems, Inc.

260 Franklin Street, Boston, Massachusetts, 02110, United States

The organization at the address above has undergone an independent audit and, at the time, was found to have met the requirements of the Standard. This certificate entitles the holder of the certificate to use this conformity mark according to the terms and conditions of the application or according to the scheme holder. To verify the status of the certificate, please feel free to contact Orion at info@orioncan.com.

MSCB-362

Certificate ID:	OR-13099-4
SOA:	Version 12
Initial Certification:	Mar 23, 2012
Issue Date:	Nov 7, 2025
Expiry Date:	Feb 20, 2027
IAF Code:	["35 Other services"]

David Huebel, President
Orion Assessment Services International Inc.
209-1201 Dundas Street East
Toronto, Ontario, M4M 1S2

SOC 2 Type 2 Report

Boostlingo LLC ("Boostlingo")

November 1, 2023 to November 1, 2024

A Type 2 Independent Service Auditor’s Report on Controls Relevant to Security, Confidentiality and Availability

AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA

Prescient Assurance LLC.
1100 Market Street Suite 600
Chattanooga, TN 37402

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319

AICPA NOTICE:

You may use the SOC for Service Organizations - Service Organizations Logo only for a period of twelve (12) months following the date of the SOC report issued by a licensed CPA. If after twelve months a new report is not issued, you must immediately cease use of the SOC for Service Organizations - Logo.

Table of Contents

Management's Assertion **6**
Independent Service Auditor's Report 9
Scope 9
Service Organization's Responsibilities 9
Service Auditors' Responsibilities 10
Inherent Limitations 10
Opinion 11
Restricted Use 11
System Description **13**
DC 1: Company Overview and Types of Products and Services Provided 14
DC 2: The Principal Service Commitments and System Requirements 15
3.1 Primary Infrastructure 16
3.2 Primary Software 17
3.3 People 17
3.3 Data 18
3.4 Processes and procedures 19
3.5.1 Physical security 20
3.5.2 Logical access 20
3.5.3 Computer operations - backups 20
3.5.4 Computer operations - availability 20
3.5.5 Change management 21
3.5.6 Data communications 21
3.6 Boundaries of the system 21
DC 4: Disclosures about Identified Security Incidents 22
DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved 23
5.1 Integrity and ethical values 23
5.2 Commitment to competence 23
5.3 Management's philosophy and operating style 24
5.4 Organizational structure and assignment of authority and responsibility 24
5.5 HR policies and practices 25
5.6 Risk assessment process 25
5.7 Integration with risk assessment 25
5.8 Information and communication systems 25
5.9 Monitoring controls 26
5.9.1 On-going monitoring 26
5.10 Reporting deficiencies 26
DC 6: Complementary User Entity Controls (CUECs) 27

DC 7: Complementary Subservice Organization Controls (CSOCs) 28
DC 8: Any Specific Criterion of the Applicable Trust Services Criteria That is Not Relevant to the System and the Reasons it is Not Relevant 30
DC 9: Disclosure of Significant Changes in Last 1 Year 31
Testing Matrices **32**
Tests of Operating Effectiveness and Results of Tests 33
Scope of Testing 33
Types of Tests Generally Performed 33
General Sampling Methodology 34
Reliability of Information Provided by the Service Organization 35
Test Results 35

SECTION 1

Management's Assertion

Management's Assertion

We have prepared the accompanying description of Boostlingo's system throughout the period November 1, 2023 to November 1, 2024, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report. The description is intended to provide report users with information about Boostlingo's system that may be useful when assessing the risks arising from interactions with Boostlingo's system, particularly information about system controls that Boostlingo has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Boostlingo uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Boostlingo, to achieve Boostlingo's service commitments and system requirements based on the applicable trust services criteria. The description presents Boostlingo's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Boostlingo's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Boostlingo, to achieve Boostlingo's service commitments and system requirements based on the applicable trust services criteria. The description presents Boostlingo's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Boostlingo's controls.

We confirm, to the best of our knowledge and belief, that:

a. The description presents Boostlingo's system that was designed and implemented throughout the period November 1, 2023 to November 1, 2024 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period November 1, 2023 to November 1, 2024, to provide reasonable assurance that Boostlingo's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Boostlingo's controls during that period.
c. The controls stated in the description operated effectively throughout the period November 1, 2023, to November 1, 2024, to provide reasonable assurance that Boostlingo's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of Boostlingo's controls operated effectively throughout the period.

DocuSigned by:
Bryan Forrester
22561D7B4941497...

Bryan Forrester
CEO
Boostlingo

SECTION 2

Independent Service Auditor's Report

Independent Service Auditor's Report

To: Boostlingo

Scope

We have examined Boostlingo LLC's ("Boostlingo") accompanying description of its Boostlingo On-Demand and Boostlingo IMS Platform system found in Section 3, titled Boostlingo System Description throughout the period November 1, 2023, to November 1, 2024, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2023, to November 1, 2024, to provide reasonable assurance that Boostlingo's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Boostlingo uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Boostlingo, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents Boostlingo's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Boostlingo's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Boostlingo, to achieve Boostlingo's service commitments and system requirements based on the applicable trust services criteria. The description presents Boostlingo's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Boostlingo's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

Boostlingo is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Boostlingo's service commitments and system requirements were achieved. In Section 1, Boostlingo has provided the accompanying assertion titled "Management's Assertion of Boostlingo" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Boostlingo is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
2. Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
4. Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
5. Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
6. Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in 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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become

inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects:

a. The description presents Boostlingo's system that was designed and implemented throughout the period November 1, 2023, to November 1, 2024, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period November 1, 2023, to November 1, 2024, to provide reasonable assurance that Boostlingo's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of Boostlingo's controls throughout the period.
c. The controls stated in the description operated effectively throughout the period November 1, 2023, to November 1, 2024, to provide reasonable assurance that Boostlingo's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Boostlingo's controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of Boostlingo, user entities of Boostlingo's system during some or all of the period November 1, 2023 to November 1, 2024, business partners of Boostlingo subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

1. The nature of the service provided by the service organization.
2. How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
3. Internal control and its limitations.
4. Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

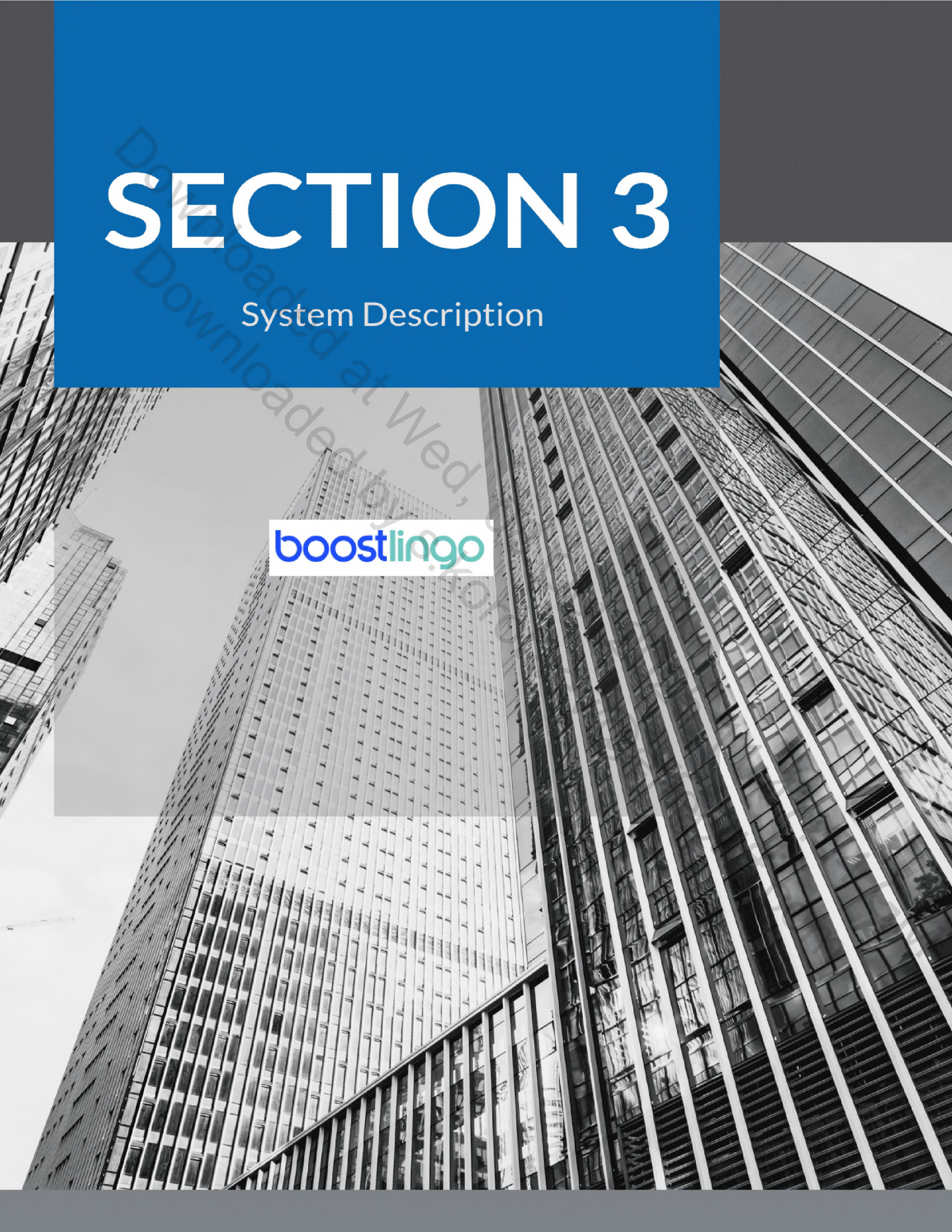
This report is not intended to be, and should not be, used by anyone other than these specified parties.

DocuSigned by:
Prescient Assurance
D4EE46AA29744B4...

Prescient Assurance LLC
February 5, 2025

SECTION 3

System Description



DC 1: Company Overview and Types of Products and Services Provided

Company Background

Boostlingo is a technology company headquartered in Austin, TX, with offices in San Francisco, Copenhagen, and Dublin. Our mission is to build innovative technology that empowers our customers and the people they serve to communicate without barriers and increase language access for all.

Description of services overview or services provided

Boostlingo simplifies language services with its all-in-one platform. From scheduling on-site, remote, and on-demand interpreters to event interpreting, AI-powered captioning, and translation services, Boostlingo provides a complete solution.

Boostlingo On-Demand allows customers to manage and deliver interpretation services through phone and video. The system description in this report section details the Boostlingo On-Demand Platform. Any other Boostlingo services are not within the scope of this report.

Boostlingo On-Demand Platform focuses on phone and video interpreting delivery and management. Customers can add staff interpreters or access the Boostlingo Hub for on-demand and pre-scheduled calls to 17,000 interpreters in 300+ languages. Intelligent routing, custom IVR, and call settings can be used for specialized call routing. In addition, customers can use detailed reporting for internal management and leverage built-in integrations.

Boostlingo IMS automates the day-to-day coordination and management of interpretation services. The platform allows for remote and on-site services to be scheduled and managed from one place.

DC 2: The Principal Service Commitments and System Requirements

Boostlingo designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Boostlingo makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Boostlingo has established for the services. The system services are subject to the Security, Confidentiality, and Availability commitments established internally for its services.

Boostlingo's commitments to users are communicated through Service Level Agreements (SLAs), Cloud Service Agreements (CSA), Master Agreements (MA), and online Privacy Policy.

Security Commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Up time availability of production systems

Confidentiality Commitments

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties
- Confidential information must be used only for the purposes explicitly stated in agreements between Boostlingo and user entities

Availability Commitments

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components
- Responding to customer requests in a reasonably timely manner
- Operational procedures supporting the achievement of availability commitments to user entities

DC 3: The Components of the System Used to Provide the Services

The System is comprised of the following components:

- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data - The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures - The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

3.1 Primary Infrastructure

Boostlingo maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers).

Hardware	Type	Purpose
AWS Elastic Compute Cloud (EC2)	AWS	FreePBX/Asterisk server used to proxy Twilio to Twilio SIP traffic
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
AWS Elastic Container Service (ECS)	AWS	Scalable, containerized deployment and orchestration of our SaaS application, ensuring high availability

3.2 Primary Software

Boostlingo is responsible for managing the development and operation of the Boostlingo On-Demand & IMS Platform system including infrastructure components such as servers, databases, and storage systems. The in-scope Boostlingo infrastructure and software components are shown in the table provided below:

System/Application	Operating System	Purpose
GuardDuty	AWS	Security application used for automated intrusion detection (IDS)
Datadog	Datadog	Monitoring application used to provide monitoring, alter, and notification services for Boostlingo platform
Redis	Linux	Used to maintain cached data
Amazon Web Services	AWS	Infrastructure in which application runs and data resides
Atlassian	Atlassian	Jira helps us track, manage, and prioritize tasks, bugs, and development workflows to streamline project execution. Confluence serves as a centralized knowledge base for documentation, collaboration, and information sharing across teams.
Datadog	Datadog	Provides real-time monitoring, logging, and observability for our infrastructure and applications, enabling proactive issue detection and performance optimization.
Elastic	Elastic	Powers search
GitHub	Github	Enables version control, collaboration, and code management for our development teams, ensuring secure and efficient software delivery.
Jira	Atlassian	Robust issue and bug tracking capabilities; project management
Office 365	Office 365	Productivity and collaboration tools and document management
Pulumi	Pulumi	Infrastructure as code (IaC), allowing us to provision, manage, and scale cloud resources with automation and consistency.

Microsoft SQL Server	Windows Server (AWS RDS)	Relational data storage

3.3 People

Boostlingo employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. Boostlingo focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Boostlingo has a staff of approximately 160 organized in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.
This includes:

- CEO - Bryan Forrester
- CFO - Scott Parnell
- CTO - Matt Cotton
- CRO - Merrie Wallace
- CPO - Nina Siglin
- VP of Product - Brian D'Agostino
- VP of Language Access - Caroline Remer

Operations: Responsible for maintaining the availability of production infrastructure, and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Technology: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

3.3 Data

Data as defined by Boostlingo, constitutes the following:

User and Account Data - this includes personally identifiable information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system

permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized in the following major types of data used by Boostlingo

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Boostlingo.	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by Boostlingo. Boostlingo must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Boostlingo to operate the business. Boostlingo must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by Boostlingo in delivering its services.

All personnel and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Boostlingo has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

3.4 Processes and procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, control owners, and Legal. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

3.5.1 Physical security

Boostlingo's production servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. Boostlingo reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

3.5.2 Logical access

Boostlingo provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems is split into admin roles, user roles, and no access roles. User access and roles are reviewed on an annual basis to ensure least privilege access.

IT is responsible for provisioning access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Boostlingo's policies, completing security training. These steps must be completed within thirty (30) days of hire.

When an employee is terminated, IT is responsible for deprovisioning access to all in scope systems within 24 hours of that employee's termination.

3.5.3 Computer operations - backups

Customer data is backed up and monitored by the DevOps Team for completion and exceptions. If there is an exception, DevOps Team will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

3.5.4 Computer operations - availability

Boostlingo maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting and acting upon breaches or other incidents.

Boostlingo internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Boostlingo utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open source dependencies and maintains an internal SLA for responding to those issues.

3.5.5 Change management

Boostlingo maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

3.5.6 Data communications

Boostlingo has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Boostlingo application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

Boostlingo uses an automated monitoring service to perform vulnerability scans and engages an external firm to perform annual penetration testing to look for unidentified vulnerabilities, and the engineering team responds to any issues identified via the regular incident response and change management process.

3.6 Boundaries of the system

The boundaries of the Boostlingo On-Demand & IMS Platform are the specific aspects of the Company's

infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Boostlingo On-Demand & IMS Platform.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

DC 4: Disclosures about Identified Security Incidents

No significant incidents have occurred to the services provided to user entities during the review period or since the Boostlingo's last review.

DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

5.1 Integrity and ethical values

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

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee handbook (and associated policies) and understand their responsibility for adhering to the policies and procedures contained within the handbook.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

5.2 Commitment to competence

Boostlingo's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

5.3 Management's philosophy and operating style

The Boostlingo management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Boostlingo can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Boostlingo to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management and senior leadership meetings are held to discuss major initiatives and issues that affect the business.

5.4 Organizational structure and assignment of authority and responsibility

Boostlingo'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.

Boostlingo'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.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

5.5 HR policies and practices

Boostlingo'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. Boostlingo'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 acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Performance evaluations for each employee are conducted on an annual basis.
- Personnel termination procedures are in place to guide the termination/offboarding process and are documented in an offboarding checklist.

5.6 Risk assessment process

Boostlingo's risk assessment process identifies and manages risks that could potentially affect Boostlingo's ability to provide reliable and secure services to our customers. As part of this process, Boostlingo maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Boostlingo product development process so they can be dealt with predictably and iteratively.

5.7 Integration with risk assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Boostlingo's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Boostlingo 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, Boostlingo's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

5.8 Information and communication systems

Information and communication are an integral component of Boostlingo's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Boostlingo uses several information and communication channels internally to share information

with management, employees, contractors, and customers. Boostlingo uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Boostlingo uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

5.9 Monitoring controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Boostlingo's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

5.9.1 On-going monitoring

Boostlingo'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 Boostlingo'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 Boostlingo's personnel.

5.10 Reporting deficiencies

Our internal risk management 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, and instructions for escalation are supplied to employees in company policy documents. 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.

DC 6: Complementary User Entity Controls (CUECs)

Boostlingo'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 the Trust Services Criteria related to Boostlingo's services to be solely achieved by Boostlingo control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Boostlingo's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria 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.

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

DC 7: Complementary Subservice Organization Controls (CSOCs)

Subservice organizations

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

Subservice description of services

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entities services.

Complementary Subservice Organization Controls

Boostlingo's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Boostlingo's services to be solely achieved by Boostlingo control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Boostlingo.

The following subservice organization controls have been implemented by AWS and included in this report to provide additional assurance that the trust services criteria are met.

AWS

Category	Criteria	Control
Security	CC 6.4	Physical access to data centers is approved by an authorized individual.
Security	CC 6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
Security	CC 6.4	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Security	CC 6.4	Closed circuit television camera (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
Security	CC 6.4	Access to server locations is managed by electronic access control devices.
Security	CC 7.2	AWS is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.

Category	Criteria	Control
Security	CC 7.2	AWS is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
Security	CC 7.2	AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.
Availability	A 1.2	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.
Availability	A 1.2	AWS has a process in place to review environmental and geo-political risks before launching a new region.
Availability	A 1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
Availability	A 1.2	Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
Availability	A 1.2	Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon owned data centers
Availability	A 1.2	Amazon-owned data centers have generators to provide backup power in case of electrical failure.
Availability	A 1.2	Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.

Boostlingo management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Boostlingo performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

DC 8: Any Specific Criterion of the Applicable Trust Services Criteria That is Not Relevant to the System and the Reasons it is Not Relevant

All Common Criteria/Security, Security, Confidentiality, and Availability criteria were applicable to the Boostlingo's On-Demand & IMS Platform system.

DC 9: Disclosure of Significant Changes in Last 1 Year

No significant changes have occurred to the services provided to user entities in the last year preceding the end of the review date.

SECTION 4

Testing Matrices

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to Boostlingo On-Demand and Boostlingo IMS Platform provided by Boostlingo. The scope of the testing was restricted to Boostlingo On-Demand and Boostlingo IMS, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing throughout the period November 01, 2023 to November 01, 2024.

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

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

Types of Tests Generally Performed

The table below describes the nature of our audit procedures and tests performed to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Test Types	Description of Tests
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: • Examination / Inspection of source documentation and authorizations to verify transactions processed. • Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures. • Examination / Inspection of systems documentation, configurations, and settings; and

	• Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.
Observation	Observed the implementation, application or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed if applicable.

General Sampling Methodology

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

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

The table below describes the sampling methodology utilized in our testing to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Type of Control and Frequency	Minimum Number of Items to Test (Period of Review Six Months or Less)	Minimum Number of Items to Test (Period of Review More than Six Months)
Manual control, many times per day	At least 25	At least 40
Manual control, daily (Note 1)	At least 25	At least 40
Manual control, weekly	At least 5	At least 10
Manual control, monthly	At least 3	At least 4

Manual control, quarterly	At least 2	**At least 2**
Manual control, annually	Test annually	**Test annually**
Application controls	Test one operation of each relevant aspect of each application control if supported by effective IT general controls; otherwise test at least 15	**Test one operation of each application control if supported by effective IT general controls; otherwise test at least 25**
IT general controls	Follow guidance above for manual and automated aspects of IT general controls	**Follow guidance above for manual and automated aspects of IT general controls**
Notes: 1.) Some controls might be performed frequently, but less than daily. For such controls, the sample size should be interpolated using the above guidance. Generally, for controls where the number of occurrences ranges from 50 to 250 during the year, our minimum sample size using the above table should be approximately 10% of the number of occurrences.		

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than this constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the Operating Effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

Trust ID	COSO Principle	Control Description	Test Applied by the Service Auditor	Test Results
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.	The company evaluates system capacity on an ongoing basis, and system changes are implemented to help ensure that processing capacity can meet demand.	Inspected the enabled automated log alerting to determine that the company evaluates system capacity on an ongoing basis, and system changes are implemented to help ensure that processing capacity can meet demand.	No exceptions noted.
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.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the infrastructure monitoring tool configurations to determine that the company's formal policies outlined the requirements for vulnerability management and system monitoring.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Operations Security Policy to determine that information backup requirements have been documented stating that backup copies are required to be taken regularly and restore capabilities are required to be tested periodically, not less than annually.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the	Inspected the risk management policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

	infrastructure to meet its objectives.	identified threats, and mitigation strategies for those risks.		
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company has a multi-location strategy for production environments employed to permit the resumption of operations at other company data centers in the event of loss of a facility.	Inspected the company network diagram to determine that the company has a multi-location strategy for production environments employed to permit the resumption of operations at other company data centers in the event of the loss of a facility. Inspected the company's AWS configuration dashboard for the containers to determine that the company has availability zones configured to permit the resumption of operations at other company data centers in the event of loss of a facility.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company performs periodic backups for production data. Data is backed up to a different location than the production system.	Inspected the daily backup configurations to determine that the company performs periodic backups for production data. Data is backed up to a location different from the production system.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk register to determine that the company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. Inspected the Risk Management Policy to determine that risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or	The company's databases are replicated to a	Inspected the database replication and alert configurations to determine that the	No exceptions noted.

	acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	secondary data center in real-time. Alerts are configured to notify administrators if replication fails.	company's databases are replicated to a secondary data center in real-time. Alerts are configured to notify administrators if replication fails.	
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery Plan and the annual disaster recovery tabletop exercise to determine that the company has a documented BC/DR plan and tests it at least once a year.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the business continuity plan to determine that the company had Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Operations Security Policy to determine that information backup requirements have been documented stating that backup copies are required to be taken regularly and restore capabilities are required to be tested periodically, not less than annually.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected intrusion detection system configurations to determine that the company used an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.

A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery Plan and the annual disaster recovery tabletop exercise to determine that the company has a documented BC/DR plan and tests it at least once a year.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the Data Management Policy to determine that it includes procedures to help ensure that confidential data is properly secured and restricted to authorized personnel.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the vendor list to determine that the company had maintained a vendor directory. Inspected a sample of master subscription agreement and terms of service to determine the company's written agreements with vendors and related third parties, including confidentiality and privacy commitments applicable to that entity.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to determine that internal retention and disposal procedures have been established stating that the company is required to retain data as long as the company needs its use. Additionally, the policy defines the retention periods of various data types.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments.	Inspected the Data Management Policy to determine that the company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company requires authentication to systems and applications to use unique usernames, passwords, and a valid Multi-Factor Authentication method.	Inspected the company's user access list to determine that the company requires authentication for systems and applications to use unique usernames, passwords, and a valid multi-factor authentication method.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's	The company has electronic media containing confidential	Inspected the device offboarding and media sanitation record for the device disposed off during the audit period to	No exceptions noted.

	objectives related to confidentiality.	information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	determine that the company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected the process for customer data deletion to determine that it includes a formal request process, internal coordination, review, verification, processing, confirmation, and record-keeping. and found that no customer data deletion requests were received during the audit period. Inspected the Data Management Policy to determine that it specifies secure deletion practices and retention periods for data. Inquired with the client to determine that no data deletion was requested during the audit period.	Not tested
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees.	Inspected the background check records performed for a sample of new hires to determine that the company performed background checks on new employees.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected evidence of performance evaluations performed for a sample of current employees to determine that the company managers were required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to sign a confidentiality agreement during onboarding.	Inspected the signed confidentiality agreements for a sample of new hires to determine that the company required employees to sign a confidentiality agreement during onboarding.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected the contractor agreement to determine that the company requires contractors to sign a confidentiality agreement at the time of engagement.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to acknowledge a code of	Inspected the code of conduct acknowledgment for a sample of new hires and determined that the company required	No exceptions noted.

		conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	employees to acknowledge a code of conduct at the time of hire.	
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected the contractor agreements to determine that the company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's executive leadership meets at least annually to discuss the state of the company's cybersecurity and privacy risks.	Inspected the company's board of director meeting minutes and the board of director security slides to determine that the company's board of directors is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's executive leadership has a documented policy that outlines its oversight responsibilities for internal control.	Inspected the company's information security roles and responsibilities to determine that the company's executive leadership has a documented policy that outlines its oversight responsibilities for internal control.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's executive leadership has sufficient expertise to oversee the ability to design, implement, and operate information security controls. The company engages third-party information security experts and consultants as needed.	Inspected the bio for the members of the company's executive leadership to determine that the company's executive leadership has sufficient expertise to oversee the ability to design, implement, and operate information security controls. Inspected the information security policy to determine that the company engages third-party information security experts and consultants as needed.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and	The company's executive leadership meets at least annually and maintains formal meeting minutes. The leadership includes personnel that are	Inspected the meeting minutes to determine that the company's executive leadership meets at least annually and maintained formal meeting minutes. Inspected the bio for the members of the	No exceptions noted.

	performance of internal control.	independent of the company.	company's executive leadership to determine that the company includes personnel who are independent of the company.	
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy and job descriptions to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company's executive leadership has a documented policy that outlines its oversight responsibilities for internal control.	Inspected the company's information security roles and responsibilities to determine that the company's executive leadership has a documented policy that outlines its oversight responsibilities for internal control.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the organizational chart to determine that the company maintained an organizational chart that describes the organizational structure and reporting lines.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the roles and responsibilities policy and job descriptions to determine that the roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the roles and responsibilities policy.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company performs background checks on new employees.	Inspected the background check records performed for a sample of new hires to determine that the company performed background checks on new employees.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract,	The company managers are required to complete	Inspected evidence of performance evaluations performed for a sample of	No exceptions noted.

	develop, and retain competent individuals in alignment with objectives.	performance evaluations for direct reports at least annually.	current employees to determine that the company managers were required to complete performance evaluations for direct reports at least annually.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected the security awareness training tracker to determine that the company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the roles and responsibilities policy and job descriptions to determine that the roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the roles and responsibilities policy.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected evidence of performance evaluations performed for a sample of current employees to determine that the company managers were required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the code of conduct acknowledgment for a sample of new hires and determined that the company required employees to acknowledge a code of conduct at the time of hire.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security	Inspected the roles and responsibilities policy and job descriptions to determine that the roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the roles and responsibilities	No exceptions noted.

		controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	policy.	
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected the control self-assessment and remediation activities to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the company's vulnerability findings and remediations to determine that the company has vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy and job descriptions to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for	The company has security and privacy incident response policies and procedures that are documented and	Inspected the company's incident response policy to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to	No exceptions noted.

	internal control, necessary to support the functioning of internal control.	communicated to authorized users.	authorized users.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Inspected the whistleblower hotline and anonymous communication channel to determine that the company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected the security awareness training tracker to determine that the company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Inspected the company's network diagram and product documentation site to determine that the company provides a description of its products and services to internal and external users.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the	The company communicates system changes to authorized int ernal users.	Inspected the internal communication channel and log of internal communications to determine that the company communicates system changes to authorized internal users.	No exceptions noted.

	functioning of internal control.			
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the roles and responsibilities policy and job descriptions to determine that the roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the roles and responsibilities policy.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Inspected the company's network diagram and product documentation site to determine that the company provides a description of its products and services to internal and external users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected the terms of services and privacy policy on the company website to determine that the company's security commitments were communicated to customers in Terms of Service (TOS).	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the vendor list to determine that the company had maintained a vendor directory. Inspected a sample of master subscription agreement and terms of service to determine the company's written agreements with vendors and related third parties, including confidentiality and privacy commitments applicable to that entity.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the community and support page on the company's website to determine that the company provided guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has an external-facing support system in place that allows users to report system information on	Inspected the support page on the company's website to determine that the company has provided a contact form, email, and contact numbers that users can	No exceptions noted.

		failures, incidents, concerns, and other complaints to appropriate personnel.	use to request support or report issues and incidents.	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company notifies customers of critical system changes that may affect their processing.	Inspected customer notifications to determine that the company notified customers of critical system changes that may affect their processing.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the risk register to determine that the company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and	Inspected the vendor list to determine that the company maintains a vendor directory along with its risk level. Inspected a sample of vendor compliance reviews to determine that the company has compliance security reports for critical vendors and reviews them annually.	No exceptions noted.

		privacy requirements; and - review of critical third-party vendors at least annually.		
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery Plan and the annual disaster recovery tabletop exercise to determine that the company has a documented BC/DR plan and tests it at least once a year.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk register to determine that the company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. Inspected the Risk Management Policy to determine that risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental,	Inspected the risk register to determine that the company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are	No exceptions noted.

		regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	identified and the risks are formally assessed. Inspected the Risk Management Policy to determine that risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk register to determine that the company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. Inspected the Risk Management Policy to determine that risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the configuration management system to determine that the company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration testing report to determine that the company's penetration testing was performed at least annually. Inspected evidence of remediation tickets for identified vulnerabilities in the penetration report to determine that remediation plans are developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.

CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the company's vulnerability findings and remediations to determine that the company has vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected the control self-assessment and remediation activities to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor list to determine that the company maintains a vendor directory along with its risk level. Inspected a sample of vendor compliance reviews to determine that the company has compliance security reports for critical vendors and reviews them annually.	No exceptions noted.

CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration testing report to determine that the company's penetration testing was performed at least annually. Inspected evidence of remediation tickets for identified vulnerabilities in the penetration report to determine that remediation plans are developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor list to determine that the company maintains a vendor directory along with its risk level. Inspected a sample of vendor compliance reviews to determine that the company has compliance security reports for critical vendors and reviews them annually.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected the control self-assessment and remediation activities to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the	The company has a documented risk management program in	Inspected the risk management policy to determine that the company had a documented risk management program in	No exceptions noted.

	mitigation of risks to the achievement of objectives to acceptable levels.	place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the access control policy to determine that the company's access control policy documents the requirements for adding new users; modifying users; and/or removing an existing user's access.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the secure development policy to determine that the company had a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to determine that internal retention and disposal procedures have been established stating that the company is required to retain data as long as the company needs its use. Additionally, the policy defines the retention periods of various data types.	No exceptions noted.

CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Operations Security Policy to determine that information backup requirements have been documented stating that backup copies are required to be taken regularly and restore capabilities are required to be tested periodically, not less than annually.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the code changes to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and	Inspected the secure development policy to determine that the company had a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.

		maintenance of information systems and related technology requirements.		
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's incident response policy to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the roles and responsibilities policy and job descriptions to determine that the roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the roles and responsibilities policy.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the risk register to determine that the company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor list to determine that the company maintains a vendor directory along with its risk level. Inspected a sample of vendor compliance reviews to determine that the company has compliance security reports for critical vendors and reviews them annually.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over	The company requires authentication to the "production network" to use unique usernames,	Inspected the company's user access list to determine that the company requires authentication to the "production network" to use unique usernames, passwords, and a	No exceptions noted.

	protected information assets to protect them from security events to meet the entity's objectives.	passwords, and a valid Multi-Factor Authentication (MFA) method.	valid Multi-Factor Authentication (MFA) method.	
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.	The company requires authentication to systems and applications to use unique usernames, passwords, and a valid Multi-Factor Authentication method.	Inspected the company's user access list to determine that the company requires authentication for systems and applications to use unique usernames, passwords, and a valid multi-factor authentication method.	No exceptions noted.
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.	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the Data Management Policy to determine that it includes procedures to help ensure that confidential data is properly secured and restricted to authorized personnel.	No exceptions noted.
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.	System access restricted to authorized access only	Inspected user listings to determine that system access was restricted to authorized access only.	No exceptions noted.
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.	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the network segmentation to determine that the company's network is segmented to prevent unauthorized access to customer data.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them	The company's production systems can only be remotely accessed by authorized employees via an	Inspected the security certificate of the company's website and SSL certificate configurations to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted	No exceptions noted.

	from security events to meet the entity's objectives.	approved encrypted connection.	connection.	
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.	The company restricts privileged access to databases to authorized users with a business need.	Inspected database user listings to determine that the company restricted privileged access to databases to authorized users with a business need.	No exceptions noted.
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.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the production system to determine that the company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.
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.	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected firewall user listings to determine that the company restricted privileged access to the firewall to authorized users with a business need.	No exceptions noted.
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.	The company restricts privileged access to the operating system to authorized users with a business need.	Inspected operating system user listings to determine that the company restricted privileged access to the operating system to authorized users with a business need.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to	The company restricts privileged access to the production network to authorized users with a business need.	Inspected production network user listings to determine that the company restricted privileged access to the production network to authorized users with a business need.	No exceptions noted.

	meet the entity's objectives.			
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.	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the company's Access Control Policy to determine that the company has a password policy in place and it is utilized for in-scope systems when possible. Inspected the company's password policies for in-scope systems to determine that the company requires passwords for in-scope system components to be configured according to the company's policy.	No exceptions noted.
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.	The company's datastores housing sensitive customer data are encrypted at rest.	Inspected the encryption configurations to determine that the company's datastores housing sensitive customer data are encrypted at rest.	No exceptions noted.
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.	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the company's Entra and AWS user access list to determine that the company restricts privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
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.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the user access of sample employees to determine that the company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to	The company restricts access to migrate changes to production to authorized personnel.	Inspected the user listing to determine that the company restricts access to migrate changes to production to authorized personnel.	No exceptions noted.

	meet the entity's objectives.			
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.	The company maintains a formal inventory of production system assets.	Inspected the asset inventory to determine that the company maintained a formal inventory of production system assets.	No exceptions noted.
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.	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as MFA.	Inspected the company's user access list to determine that the company requires authentication to production datastores to use authorized secure authentication mechanisms, such as MFA.	No exceptions noted.
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.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the access control policy to determine that the company's access control policy documents the requirements for adding new users; modifying users; and/or removing an existing user's access.	No exceptions noted.
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.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the access control policy to determine that the company's access control policy documents the requirements for adding new users; modifying users; and/or removing an existing user's access.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes	The company completes termination checklists to ensure that access is	Inspected the termination checklists for a sample of employees terminated during the audit period to determine that the company completed termination checklists	No exceptions noted.

	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.	revoked for terminated employees within SLAs.	to ensure that access was revoked for terminated employees within SLAs.	
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.	The company requires authentication to the "production network" to use unique usernames, passwords, and a valid Multi-Factor Authentication (MFA) method.	Inspected the company's user access list to determine that the company requires authentication to the "production network" to use unique usernames, passwords, and a valid Multi-Factor Authentication (MFA) method.	No exceptions noted.
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.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the user access of sample employees to determine that the company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
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	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the access review report to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately and required changes are tracked to completion	No exceptions noted.

	administered by the entity, user system credentials are removed when user access is no longer authorized.			
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.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the user access of sample employees to determine that the company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the termination checklists for a sample of employees terminated during the audit period to determine that the company completed termination checklists to ensure that access was revoked for terminated employees within SLAs.	No exceptions noted.
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.	The company requires authentication to the "production network" to use unique usernames, passwords, and a valid Multi-Factor Authentication (MFA) method.	Inspected the company's user access list to determine that the company requires authentication to the "production network" to use unique usernames, passwords, and a valid Multi-Factor Authentication (MFA) method.	No exceptions noted.

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.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the access control policy to determine that the company's access control policy documents the requirements for adding new users; modifying users; and/or removing an existing user's access.	No exceptions noted.
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.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the access review report to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately and required changes are tracked to completion	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the access review report to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately and required changes are tracked to completion	No exceptions noted.
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	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of	Inspected the device offboarding and media sanitation record for the device disposed off during the audit period to determine that the company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of	No exceptions noted.

	longer required to meet the entity's objectives.	destruction are issued for each device destroyed.	destruction are issued for each device destroyed.	
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.	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected the process for customer data deletion to determine that it includes a formal request process, internal coordination, review, verification, processing, confirmation, and record-keeping. and found that no customer data deletion requests were received during the audit period. Inspected the Data Management Policy to determine that it specifies secure deletion practices and retention periods for data. Inquired with the client to determine that no data deletion was requested during the audit period.	Not tested
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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the termination checklists for a sample of employees terminated during the audit period to determine that the company completed termination checklists to ensure that access was revoked for terminated employees within SLAs.	No exceptions noted.
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.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to determine that internal retention and disposal procedures have been established stating that the company is required to retain data as long as the company needs its use. Additionally, the policy defines the retention periods of various data types.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the hardening standards to determine that the company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	No exceptions noted.
CC6.6	The entity implements logical access security	The company's production systems can	Inspected the production system to determine that the company's production	No exceptions noted.

	measures to protect against threats from sources outside its system boundaries.	only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the security certificate of the company's website and cloud infrastructure provider to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspected the firewall review to determine that the company reviewed its firewall rulesets at least annually and that required changes were tracked to completion.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses firewalls and configures them to prevent unauthorized access.	Inspected the firewall configurations to determine that the company used firewalls and configured them to prevent unauthorized access.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected intrusion detection system configurations to determine that the company used an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the company's vulnerability findings and remediations to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect	The company's production systems can only be remotely	Inspected the security certificate of the company's website and SSL certificate configurations to determine that the	No exceptions noted.

	against threats from sources outside its system boundaries.	accessed by authorized employees via an approved encrypted connection.	company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company requires authentication to the "production network" to use unique usernames, passwords, and a valid Multi-Factor Authentication (MFA) method.	Inspected the company's user access list to determine that the company requires authentication to the "production network" to use unique usernames, passwords, and a valid Multi-Factor Authentication (MFA) method.	No exceptions noted.
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.	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Inspected the MDM configurations to determine that the company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	No exceptions noted.
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.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the security certificate of the company's website and cloud infrastructure provider to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
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.	The company encrypts portable devices when used.	Inspected the computer listing with encrypted hard drives to determine that the company encrypts portable and removable media devices when used.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of	The company has a formal systems development life cycle (SDLC) methodology in	Inspected the secure development policy to determine that the company had a formal systems development life cycle (SDLC) methodology in place that governs	No exceptions noted.

	unauthorized or malicious software to meet the entity's objectives.	place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	
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.	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected the antivirus configurations on current employees systems to determine that the company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	No exceptions noted.
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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the company's vulnerability findings and remediations to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the Operations Security Policy to determine that the company's formal policies outlined the requirements for vulnerability management and system monitoring for IT and Engineering departments.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently	Inspected the configuration management system to determine that the company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	No exceptions noted.

	vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	throughout the environment.		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk register to determine that the company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. Inspected the Risk Management Policy to determine that risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the code changes to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the company's vulnerability findings and remediations to determine that the company has vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
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	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability	Inspected the Operations Security Policy to determine that the company's formal policies outlined the requirements for vulnerability management and system monitoring for IT and Engineering departments.	No exceptions noted.

	affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	management; - system monitoring.		
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.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the company's vulnerability findings and remediations to determine that the company has vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
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.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the infrastructure monitoring tool configurations to determine that the company's formal policies outlined the requirements for vulnerability management and system monitoring.	No exceptions noted.
CC7.2	The entity monitors system components and	The company's penetration testing is	Inspected the penetration testing report to determine that the company's penetration	No exceptions noted.

	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.	performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	testing was performed at least annually. Inspected evidence of remediation tickets for identified vulnerabilities in the penetration report to determine that remediation plans are developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	
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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the company's vulnerability findings and remediations to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
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.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected intrusion detection system configurations to determine that the company used an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
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.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security	Inspected the company's JIRA dashboard detailing the company's security incidents filter to determine that the company has a place to log and track identified vulnerability incidents. Inquired the company that there have been no security incidents that have occurred during the observation period.	Not tested

		incident response policy and procedures.		
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.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's incident response policy to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
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.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's JIRA dashboard detailing the company's security incidents filter to determine that the company has a place to log and track identified vulnerability incidents. Inquired the company that there have been no security incidents that have occurred during the observation period.	Not tested
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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the company's vulnerability findings and remediations to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
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.	The company tests their incident response plan at least annually.	Inspected the incident response tabletop exercise to determine that the company tests their incident response plan at least annually.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand,	The company has security and privacy incident response policies and procedures that are documented and	Inspected the company's incident response policy to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to	No exceptions noted.

	contain, remediate, and communicate security incidents, as appropriate.	communicated to authorized users.	authorized users.	
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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the company's vulnerability findings and remediations to determine that the company has vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's incident response policy to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery Plan and the annual disaster recovery tabletop exercise to determine that the company has a documented BC/DR plan and tests it at least once a year.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's JIRA dashboard detailing the company's security incidents filter to determine that the company has a place to log and track identified vulnerability incidents. Inquired the company that there have been no security incidents that have occurred during the observation period.	Not tested
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company tests their incident response plan at least annually.	Inspected the incident response tabletop exercise to determine that the company tests their incident response plan at least annually.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure,	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development,	Inspected the secure development policy to determine that the company had a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including	No exceptions noted.

	data, software, and procedures to meet its objectives.	acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	emergency changes), and maintenance of information systems and related technology requirements.	
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.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the hardening standards to determine that the company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	No exceptions noted.
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.	The company restricts access to migrate changes to production to authorized personnel.	Inspected the user listing to determine that the company restricts access to migrate changes to production to authorized personnel.	No exceptions noted.
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.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the code changes to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
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.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration testing report to determine that the company's penetration testing was performed at least annually. Inspected evidence of remediation tickets for identified vulnerabilities in the penetration report to determine that remediation plans are developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.

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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the company's vulnerability findings and remediations to determine that the company has vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the company's vulnerability findings and remediations to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the business continuity plan to determine that the company had Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected the cybersecurity insurance policy to determine that the company maintained cybersecurity insurance to mitigate the financial impact of business disruptions.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed.	Inspected the risk register to determine that the company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. Inspected the Risk Management Policy to determine that risk assessment includes a	No exceptions noted.

		The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	consideration of the potential for fraud and how fraud may impact the achievement of objectives.	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor list to determine that the company maintains a vendor directory along with its risk level. Inspected a sample of vendor compliance reviews to determine that the company has compliance security reports for critical vendors and reviews them annually.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the vendor list to determine that the company had maintained a vendor directory. Inspected a sample of master subscription agreement and terms of service to determine the company's written agreements with vendors and related third parties, including confidentiality and privacy commitments applicable to that entity.	No exceptions noted.

AgileSecOps, LLC

HIPAA Attestation of Compliance

Version 1.1

Boostlingo engaged AgileSecOps, LLC to perform an assessment against HIPAA to determine Boostlingo's current level of compliance against the current standard.

The compliance levels are labeled as either Compliant (Green Circle), Needs Improvement (Yellow Circle), or Not-Compliant (Red Circle).

AgileSecOps performed the inspection of Boostlingo's controls between 05/05/2024 and 07/28/2024.

The following was created from the HIPAA regulation 45 CFR Part 164. It covers the Standards, Required items, and Addressable items.

Overall, we find Boostlingo in compliance with the HIPAA regulation based on our examination of their policies, procedures, and controls.

#	CFR §	S / R / A *	Safeguard	Status	Control
1	164.308 (a)(1)(i) *Security Management Process*	S	Implement policies and procedures to prevent, detect, contain, and correct security violations.		Boostlingo has an Information Security Policy that sets the baseline for section 164.308
2	164.308 (a)(1)(ii)(A) *Risk Analysis*	R	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity.		Boostlingo has completed a Risk Assessment within the last 12 months.
3	164.308 (a)(1)(ii)(B) *Risk Management*	R	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).		Boostlingo has implemented security measures to reduce risk within its Information Security Policy and 'Vulnerability and Penetration Testing Management Policy
4	164.308 (a)(1)(ii)(C) *Sanction Policy*	R	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.		Boostlingo has a sanction policy outlined within their Disciplinary Policy
5	164.308 (a)(1)(ii)(D) *Information System Activity Review*	R	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.		Boostlingo has a Logging and Monitoring policy that speaks to logging activity requirements, system/logging review, and security exception reporting.
6	164.308 (a)(2)	S	Identify the security official responsible for the development		Joe Bagdon (acting CISO) and Noelle Lattimore (VP of Legal and Compliance) are responsible for the development and

	Assigned Security Responsibilities		and implementation of the policies and procedures required by this subpart for the entity.		implementation of the policies and procedures required by HIPAA.
7	164.308 (a)(3)(i) *Workforce Security*	S	Implement policies and procedures to ensure that all members of its workforce have appropriate access to ePHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) from obtaining access to ePHI.		Boostlingo has an Access Control Policy that has policies and procedures to ensure only those with the need to know have continued access to the production environment.
8	164.308 (a)(3)(ii)(A) *Authorization and/or Supervision*	A	Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.		Boostlingo has an Access Control Policy that has procedures for the authorization of employees that need access to the production environment which contains ePHI.
9	164.308 (a)(3)(ii)(B) *Workforce Clearance Procedure*	A	Implement procedures to determine that the access of a workforce member to ePHI is appropriate.		Boostlingo has an Access Control Policy that has procedures to ensure that access into the production environment that contains ePHI is appropriate.
10	164.308 (a)(3)(ii)(C) *Termination Procedures*	A	Implement procedures for terminating access to ePHI when the employment of a workforce member ends, or as required by paragraph (a)(3)(ii)(B) of this section.		Boostlingo has an Access Control Policy that has procedures to terminate access when either employment is terminated or when access is no longer needed.
11	164.308 (a)(4)(i) *Information Access*	S	Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable		Boostlingo has an Access Control Policy that has policies and procedures to ensure only those with the need to know have continued access to the production environment.

	Management		requirements of subpart E of this part (the Privacy Rule).		
12	164.308 (a)(4)(ii)(B) *Access Authorization*	A	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.		Boostlingo has an Access Control Policy that has policies and procedures to ensure only those with the need to know have continued access to the production environment which contains ePHI. Access is granted through the individual's workstation and access into the production environment through a VPN connection.
13	164.308 (a)(4)(ii)(C) *Access Establishment and Modification*	A	Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.		Boostlingo has an Access Control Policy that has policies and procedures to ensure that there is a review period for all access and the policies and procedures.
14	164.308 (a)(5)(i) *Security Awareness and Training*	S	Implement a security awareness and training program for entire workforce (including management).		Security awareness training is provided upon hire and annually through KnowBe4 and is outlined in the Personnel Security Policy
15	164.308 (a)(5)(ii)(A) *Security Reminders*	A	Periodic security updates are completed.		The Boostlingo Information Security Policy talks to how periodic security training updates are provided to the company.
16	164.308 (a)(5)(ii)(B) *Protection From Malicious Software*	A	Procedures for guarding against, detecting, and reporting malicious software exist.		The Boostlingo Information Security Policy and Acceptable Use Policy speak to the procedure of guarding against, detecting, and reporting on malicious software as well as other security issues.
17	164.308 (a)(5)(ii)(C) *Log-In Monitoring*	A	Procedures exist for monitoring log-in attempts and reporting discrepancies.		Boostlingo has a Logging and Monitoring Policy that speaks to logging activity requirements, system/logging review, and security exception reporting. Boostlingo actively monitors log-in attempts and reports on any discrepancies.

18	164.308 (a)(5)(ii)(D) *Password Management*	A	Procedures exist for creating, changing, and safeguarding passwords.		The Acceptable Use Policy speaks to the procedure of creating, changing, and safeguarding passwords.
19	164.308 (a)(6)(i) *Security Incident Procedures*	S	Implement policies and procedures to address security incidents.		Boostlingo has a comprehensive incident handling guide (Boostlingo Incident Management Policy) that deals with the policies and procedures needed to handle an incident within the environment.
20	164.308 (a)(6)(ii) *Response and Reporting*	R	Identify and respond to suspected or known security incidents. Mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity. Document security incidents and their outcomes.		The Information Security Policy speaks to the procedure of Exception Reporting and the Boostlingo Incident Management Policy has detailed instructions on Response and Reporting.
21	164.308 (a)(7)(i) *Contingency Plan*	S	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems containing ePHI.		Boostlingo has a Business Continuity and Disaster Recovery Policy that considers the need for a BIA, planning, and testing of procedures to recover from a disaster or other major event.
22	164.308 (a)(7)(ii)(A) *Data Backup Plan*	R	Establish and implement procedures to create and maintain retrievable exact copies of ePHI.		Boostlingo has a Backup and Restoration Policy that includes backup procedure and retention policy.
23	164.308 (a)(7)(ii)(B) *Disaster Recovery Plan*	R	Establish (and implement as needed) procedures to restore any loss of data.		Boostlingo has a Contingency Plan. Boostlingo additionally has internal Disaster Recovery Procedures.

24	164.308 (a)(7)(ii)(C) *Emergency Mode Operation Plan*	R	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of ePHI while operating in emergency mode.		Boostlingo has a Contingency Plan. Boostlingo also has their Access Control Policy that speaks to emergency system access.
25	164.308 (a)(7)(ii)(D) *Testing and Revision Procedures*	A	Implement procedures for periodic testing and revision of contingency plans.		Boostlingo has a Contingency Plan, and the plan incorporates periodic testing.
26	164.308 (a)(7)(ii)(E) *Application and Data Criticality Analysis*	A	Assess the relative criticality of specific applications and data in support of other contingency plan components.		Boostlingo has a Contingency Plan. The plan does address the criticality of applications and what is needed for Boostlingo to operate efficiently.
27	164.308 (a)(8) *Evaluation*	S	Perform a periodic technical and nontechnical evaluation based initially upon the standards implemented under this rule and subsequently in response to environmental or operational changes affecting the security of ePHI. Evaluation should establish the extent to which an entity's security policies and procedures meet the requirements of this subpart.		Boostlingo performs regular reviews of policies, procedures, technical, and nontechnical aspects of HIPAA controls at least annually or when there is a material change in the Boostlingo environment.
28	164.308 (b)(1) *Business Associate Contracts and Other*	S	A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit ePHI on the covered		Boostlingo currently does not have any Business Associates.

	Arrangements		entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information.		
29	164.308 (b)(4) *Written Contract or Other Arrangement*	R	Document the satisfactory assurances required by paragraph (b)(1) [the Business Associate Contracts and Other Arrangements] of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).		Boostlingo currently does not have any Business Associates. However, they do understand that a signed BAA would be required as an arrangement in a contract.
30	164.310 (a)(1) *Facility Access Controls*	S	Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.		Boostlingo's data center SOC 2 report has been reviewed to ensure there are adequate Facility Access Controls in place.
31	164.310 (a)(2)(i) *Contingency Operations*	A	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.		Boostlingo has a Contingency Plan. Boostlingo additionally has internal Disaster Recovery Procedures. The combination of the Boostlingo Contingency Plan and internal Disaster Recovery Procedures cover access and restoring lost data.

32	164.310 (a)(2)(ii) *Facility Security Plan*	A	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.		Boostlingo's data center SOC 2 report has been reviewed to ensure there are adequate security controls in place to prevent unauthorized physical access, tampering, and theft.
33	164.310 (a)(2)(iii) *Access Control and Validation Procedures*	A	Implement procedures to control and validate people's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision.		Boostlingo's data center SOC 2 report has been reviewed to ensure there are adequate Facility Access Controls in place.
34	164.310 (a)(2)(iv) *Maintenance Records*	A	Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks).		Boostlingo's data center SOC 2 report has been reviewed to ensure there is documentation and adequate oversight regarding repairs and modifications to the physical components of the physical security.
35	164.310 (b) *Workstation Use*	S	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.		The Boostlingo Acceptable Use Policy speaks to the procedure of proper use of workstations and security surrounding ePHI.
36	164.310 (c) *Workstation Security*	S	Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.		The Boostlingo Acceptable Use Policy speaks to the procedure and policy surrounding the physical safeguarding of workstations that have access to ePHI.

37	164.310 (d)(1) *Device and Media Controls*	S	Implement policies and procedures that govern the receipt and removal of hardware and electronic media containing ePHI into, out of, and within a facility.		Boostlingo has a Data Protection Policy that specifies that hardware / media will be inventoried and tracked.
38	164.310 (d)(2)(i) *Disposal*	R	Implement policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored.		Boostlingo has a Data Retention and Disposal Policy that specifies the procedures for disposal of media.
39	164.310 (d)(2)(ii) *Media Re-use*	R	Implement procedures for removal of ePHI from electronic media before the media are made available for reuse.		Boostlingo has a Technology Equipment Handling and Disposal Policy that specifies the procedures for reuse of media.
40	164.310 (d)(2)(iii) *Accountability*	A	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.		Boostlingo has a Data Protection Policy that specifies that hardware / electronic media will be tracked, and roles / responsibilities are defined
41	164.310 (d)(2)(iv) *Data Backup and Storage*	A	Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.		Boostlingo has a Backup and Restoration Policy that takes into consideration taking full backups on a regular basis, testing backups, and prior to decommissioning servers.
42	164.312 (a)(1) *Access Control*	S	Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).		Boostlingo has an Access Control Policy that mandates the use of a unique name and user ID for each individual to only allow access to those with the need to know to the production environment.

43	164.312 (a)(2)(i) *Unique User Identification*	R	Assign a unique name and/or number for identifying and tracking user identity.		Boostlingo has an Access Control Policy that mandates the use of a unique name and user ID for each individual.
44	164.312 (a)(2)(ii) *Emergency Access Procedure*	R	Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.		Boostlingo has an Access Control Policy and Key Management and Cryptography Policy that has policy and procedure for obtaining emergency access to the production environment.
45	164.312 (a)(2)(iii) *Automatic Logoff*	A	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.		Boostlingo has a Network Security Policy that mandates that all sessions need to be terminated after a period of inactivity.
46	164.312 (a)(2)(iv) *Encryption and Decryption*	A	Implement a mechanism to encrypt and decrypt ePHI.		Boostlingo has a Key Management and Cryptography Policy that states that all raw data will be encrypted at rest and in flight. Boostlingo currently encrypts data in transit over public networks with TLS encryption. All raw data in the Boostlingo application database will be encrypted in accordance with the Boostlingo Encryption policy.
47	164.312 (b) *Audit Controls*	S	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems containing or using ePHI.		Boostlingo has a Logging and Monitoring Policy that states procedures for the review of logs to ensure no malicious activities are taking place.
48	164.312 (c)(1) *Integrity*	S	Implement policies and procedures to protect ePHI from improper alteration or destruction.		Boostlingo's Access Control Policy only allows individuals with the need to know, have been background checked, and have supervisor approval to have access into the production environment. Additionally, in accordance with Boostlingo's Backup Policy, all customer data is backed up to geographically different locations daily.

49	164.312 (c)(2) *Mechanism to Authenticate ePHI*	A	Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.		To satisfy this requirement, Boostlingo will perform periodic checks of system and application access logs for any unauthorized access. All potential incidents will be investigated by the Boostlingo Security Team.
50	164.312 (d) *Person or Entity Authentication*	S	Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.		Boostlingo's Access Control Policy only allows individuals with the need to know, have been background checked, and have supervisor approval to have access into the production environment. Individuals are then granted with credentials that can only be used for and are tied to the individual.
51	164.312 (e)(1) *Transmission Security*	S	Implement technical security measures to guard against unauthorized access to ePHI being transmitted over an electronic communications network.		All Boostlingo communications take place, over the Internet, within a TLS encrypted tunnel.
52	164.312 (e)(2)(i) *Integrity Controls*	A	Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.		All sensitive data that is transmitted over public or non-trusted networks is encrypted with TLS encryption. This ensures the integrity and privacy of the data in transit.
53	164.312 (e)(2)(ii) *Encryption*	A	Implement a mechanism to encrypt ePHI whenever deemed appropriate.		Boostlingo's Key Management and Cryptography Policy states that all raw data will be encrypted at rest and in flight. Boostlingo currently encrypts data in transit over public networks with TLS encryption. All raw data in the Boostlingo application database will be encrypted in accordance with the Boostlingo Encryption policy.
54	164.314 (a)(1)(i) *Business Associate Contracts or Other Arrangements*	S	The contract or other arrangement between the covered entity and its business associate required by §164.308(b) must meet the requirements of paragraph (a)(2)(i) or		Boostlingo has developed a standard BAA. This BAA is compliant with this section and all that is referenced in this section.

			(a)(2)(ii) of this section, as applicable.		
55	164.314 (a)(1)(ii)(A) *Business Associate Contracts or Other Arrangements Non-Compliance*	R	A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful— Terminated the contract or arrangement, if feasible; or		Boostlingo has developed a standard BAA. After review of the BAA it has been determined to cover material breach and termination of contract.
56	164.314 (a)(1)(ii)(B) *Business Associate Contracts or Other Arrangements Non-Compliance*	R	If termination is not feasible, reported the problem to the Secretary.		Boostlingo has developed a standard BAA. After review of the BAA it has been determined to cover reporting the problem to the Secretary.
57	164.314 (a)(2)(i)(A,B,C,D) *Business Associate Contracts*	R	Business Associate Contracts must provide that the business associate will: (A) Implement administrative, physical, and technical safeguards		Boostlingo has developed a standard BAA. After review of the BAA it has been determined to cover all aspects of this section to include A, B, C, and D.

			that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity...; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.		
58	164.316 (a) *Policies and Procedures*	S	Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be		Boostlingo has policies and procedures that satisfy this requirement. These policies include the Boostlingo Security Policy, Risk Assessment, and Boostlingo's BAA.

			construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.		
59	164.316 (b)(1)(i) *Documentation*	S	Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form.		Boostlingo maintains all HIPAA policies and procedures online within their GRC platform.
60	164.316 (b)(1)(ii) *Documentation*	S	If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.		Boostlingo has a section in the Internal Audit Policy to document any assessments and findings.
61	164.316 (b)(2)(i) *Time Limit*	R	Retain the documentation required by paragraph (b)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.		Boostlingo has a Data Retention and Disposal Policy that outlines all documents pertaining to Boostlingo's policies and procedures dealing with HIPAA compliance will be retained for at least a period of 6 years
62	164.316 (b)(2)(ii) *Availability*	R	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.		All Boostlingo documents and procedures are kept on a central repository for all applicable users.

63	164.316 (b)(2)(iii) *Updates*	R	Review documentation periodically and update as needed in response to environmental or operational changes affecting the security of the ePHI.		All documents and procedures are reviewed at least annually and/or updated when needed.

Auditing Team Credentials

Qualifications and Certifications

- 30 years of experience providing digital Security and Administration
- 13 years with the DoD performing Network Defense and Network Attack
- Cybersecurity Maturity Model Certification (CMMC) - Lead Penetration Tester
- FedRAMP – Auditor and Penetration Tester
- Certifications obtained (current and previous):
  - Certified Information Systems Security Professional (CISSP)
  - HITRUST Certified CSF Practitioner (CCSFP)
  - Information Systems Security Architecture Professional (ISSAP)
  - Payment Card Industry Qualified Security Assessor (PCI QSA)
  - Global Computer Incident Response Team (GCIRT) manager
  - ISSAP (Information Systems Security Architecture Professional)
  - CIFI (Certified Information Forensics Investigator)
  - AWS Business Professional
  - AWS Technical Professional
  - GIAC Certified Incident Handler (GCIH)
  - GIAC Security Essentials (GSEC)
- Courses taken:
  - SANS Security 401 - Security Essentials
  - SANS Security 502 - Perimeter Protection In-Depth
  - SANS Security 504 - Hacker Techniques, Exploits and Incident Handling
  - SANS Security 542 - Web App Penetration Testing and Ethical Hacking
  - Programming for Everybody (Python)
  - An Introduction to Interactive Programming in Python