

EVALUATION SECTION 1: COMPANY QUALIFICATIONS AND EXPERIENCE

Company Overview

Provide a brief description of your company, including years in business, ownership structure, primary service lines relevant to AI translation and language access, number of public sector clients, and any government-specific certifications or cooperative contract experience.

BIG Language Solutions is a privately held company that provides AI-enabled language access support and business services, headquartered in Atlanta, Georgia. Founded in 2019, BIG was created to meet the growing communication, compliance, and multilingual engagement needs of highly regulated industries, including government and public sector, healthcare and life sciences, education, legal and compliance, finance and banking, energy and utilities, and other mission-critical environments.

Although BIG was formally established in 2019, our organization brings together a family of specialized language service providers with decades of proven experience, including Language Link, ISI Language Solutions, Protranslating, Paras & Associates, and other experienced providers. This structure gives BIG the scale, technology, quality systems, and national reach of an enterprise provider, while preserving the specialized expertise, client familiarity, and service responsiveness of long-standing language access organizations.

BIG provides AI-enabled translation, interpretation, and language access workflows in more than 300 languages and dialects. Our services are delivered through a global network of professional linguists, project managers, interpreters, technologists, and compliance-focused support teams. We are experienced in supporting public agencies that must communicate clearly, accurately, and equitably with limited English proficient individuals, while meeting strict requirements for confidentiality, accessibility, data security, and regulatory compliance.

Primary service lines relevant to AI-enabled translation and language access

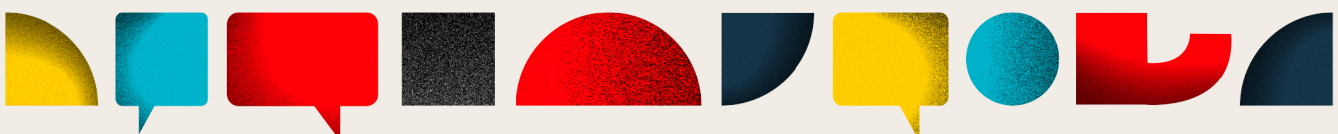
BIG delivers a comprehensive suite of language access services aligned with the needs of municipalities, public agencies, educational institutions, healthcare organizations, and other regulated entities. Our relevant service lines include:

- Written document translation for public notices, forms, benefits materials, legal communications, educational content, healthcare communications, emergency messaging, websites, digital content, and public-facing outreach.
- Over-the-phone interpretation, video remote interpretation, and onsite interpretation for public-sector, healthcare, social services, legal, education, and community engagement settings.
- AI-assisted translation workflows supported by human linguist review, terminology management, translation memory, quality assurance, and secure handling of sensitive information.



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



- AI-enabled interpretation for meetings, conferences, administrative and low-stakes calls/encounters, driven by custom interpretation engines with human-interpreter escalation as standard.
- Real-time and near-real-time multilingual communication tools for digital content, high-volume translation, and time-sensitive public communications.
- Language access program support, including workflow design, reporting, account management, quality monitoring, and scalable staffing for high-demand periods.

BIG integrates advanced AI-driven tools into our language service workflows, including custom machine translation engines, tailored transcription and transcreation tools, terminology management, quality estimation, and proprietary solutions for PHI/PII redaction. Our approach is intentionally human-centered: AI is used to improve speed, consistency, scalability, and cost efficiency, while experienced linguists, editors, and quality teams provide the oversight needed for accuracy, cultural relevance, risk mitigation, and compliance.

BIG's portfolio of AI-enabled language access solutions includes:

- **LanguageExpress™:** Our high-volume, rapid translation workflow, originally developed for healthcare, leverages neural machine translation (NMT) and AI to process thousands of files in hours. It integrates seamlessly into client systems, supporting urgent or time-critical communications.
- **LanguageNow™:** Our real-time solution for secure, instant translation of digital content, leveraging custom engines. LanguageNow™ delivers immediate, reliable results for organizations that require always-on multilingual support.
- **AI Interpreter for Meetings:** Our AI-powered simultaneous interpretation solution delivers real-time multilingual voice translation for meetings, conferences, and live events. Using advanced speech recognition, neural machine translation (NMT), and AI voice technology, the AI Interpreter for Meetings enables seamless communication across languages with low latency and integration with major conferencing platforms.
- **AI Interpreter for Conversations:** Our AI-powered conversational interpretation solution provides instant multilingual communication for call/contact center environments or encounters where an interpreter would typically be used for a 1:1 conversation. Designed for everyday, low-stakes conversations, the AI Interpreter for Conversations enables fast, natural dialogue across languages.

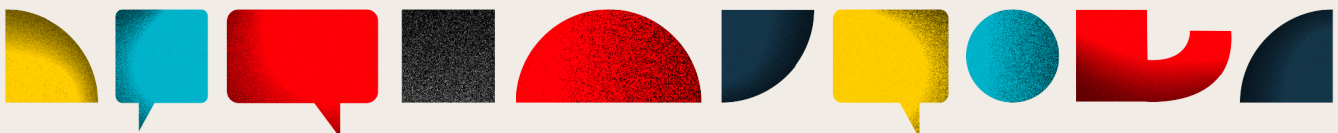
Number of public sector clients

BIG Language Solutions has extensive experience supporting government clients at federal, state, and local levels and is currently working with over 3,500 government clients. Below are examples of government clients we are currently working with.



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



- New York State Department of Taxation and Finance
- New Mexico Human Services Department
- Department of Health and Human Services
- WA ESD
- WA Department of Labor & Industry
- Income Maintenance Program
- WA DOH
- Alabama Department of Public Health
- Oregon DHS-SSP
- Idaho Health & Welfare
- Region 2- King South (Kent) CSO
- Oregon DHS
- Region 2- White Center CSO
- NJ State - Department of Children & Families
- OEP – Oregon Eligibility Partnership
- Florida Department of Elder Affairs
- State of Utah Dept Workforce Services

Government-specific certifications

BIG maintains a broad network of qualified linguists, interpreters, editors, and reviewers with experience in regulated and public-sector environments. Many of our linguists hold professional certifications, credentials, memberships, or specialized qualifications, including:

- Washington Department of Social and Health Services (DSHS) certification
- American Translators Association (ATA) certification
- Federal and State Court Interpreter certification
- International Association of Professional Translators and Interpreters (IAPTI) membership
- Institute of Translation and Interpreting (ITI) membership
- Society of Translators and Interpreters of British Columbia certification
- Department of Defense security clearance, where applicable
- Bridging the Gap Medical Interpretation certification.

Cooperative contract experience

BIG and its affiliate organizations have substantial experience supporting government agencies through state contracts, public-sector procurement vehicles, and cooperative purchasing arrangements. This experience allows BIG to respond effectively to the administrative, reporting, pricing, compliance, and performance expectations associated with public-sector contracts.

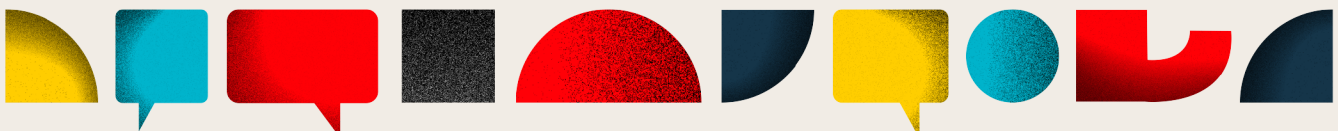
Government and Cooperative Purchasing Vehicles

BIG's affiliate company, Language Link, holds the schedules below.



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



- California Department of General Services (CADGS) for translation and interpretation services.
- New York State Office of General Services (NYOGS)

State Contracts:

- California DCSS/LCSA #30-1061
- Department of State of Hospitals
- California Dept of Health Care
- County of Orange, Dept of Mental Health
- New York State Department of Taxation and Finance
- New Mexico Human Services Department
- Department of Health and Human Services
- WA ESD
- WA Department of Labor & Industry
- WA DOH
- Alabama Department of Public Health
- Oregon DHS-SSP
- Idaho Health & Welfare
- Oregon DHS
- NJ State - Department of Children & Families
- State of Utah Dept Workforce Services

GPOs

- National Association of State Procurement Officials (NASPO)
- Massachusetts Operational Services Division (OSD)

BIG understands that successful cooperative contracts require more than service delivery. They require transparent pricing, responsive implementation, strong reporting, contract compliance, scalable support, and the ability to serve agencies of varying sizes and needs. BIG's public-sector experience, national delivery model, AI-enabled workflows, human quality oversight, and established government client base position us to deliver immediate value

AI Technology and Platform

Describe the AI technology underlying your translation and interpretation services. Address the following:

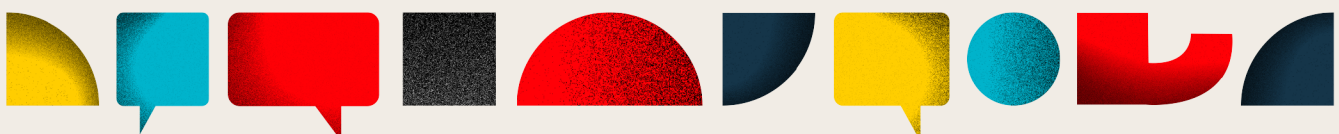
- **Underlying AI/ML architecture (e.g., neural machine translation, large language models, speech-to-text ASR models)**

BIG's AI-assisted translation platform is primarily built on neural machine translation models using sequence-to-sequence Transformer architectures. These models use attention mechanisms to evaluate context across the full source segment and generate target-language output that reflects meaning,



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



terminology, tone, and linguistic structure more accurately than legacy rule-based or phrase-based translation systems.

For written translation, BIG's AI-enabled workflow may include:

- Neural machine translation for high-volume and time-sensitive content.
- Translation memory matching to reuse previously approved human translations.
- Terminology and glossary enforcement for agency-specific vocabulary.
- Quality estimation to identify segments that require additional review.
- AI-assisted post-editing support for consistency, formatting, and fluency.
- Human linguist review and post-editing where required by content type, risk level, client preference, or regulatory sensitivity.

For live and real-time interpretation use cases, BIG uses a modular speech-to-speech architecture that can include:

- Streaming automatic speech recognition to convert spoken language into text.
- Neural machine translation to render the source language into the selected target language.
- Text-to-speech output, captions, subtitles, or transcript generation depending on the meeting format.
- Web-based or application-based participant access for multilingual audiences.
- Integration pathways for common virtual meeting environments and client systems.
- Escalation to a human interpreter, when required, in conversations.

This architecture allows BIG to support multilingual communication across live meetings, digital environments, call centers, public-facing documents, and high-volume translation workflows.

- [Whether your AI models are proprietary, open-source, or built on third-party foundations \(e.g., GPT, Whisper, DeepL, Google Translate API\)](#)

BIG uses a flexible model strategy that allows us to match the technology stack to each client's risk profile, security requirements, language needs, and content sensitivity.

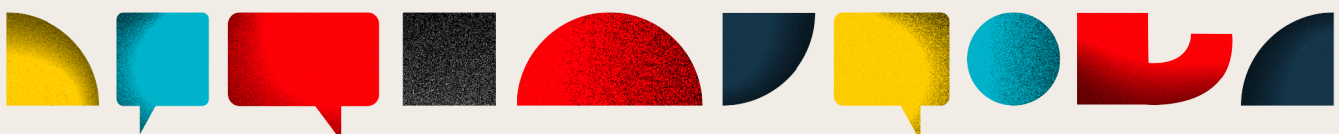
The majority of BIG's translation workflows are supported by proprietary and internally configured machine translation resources, trained or tuned using curated domain-specific and client-specific language assets, including approved translation memories, glossaries, and historical human translations. For select auxiliary tasks, such as automatic post-editing, quality enhancement, summarization support, or low-resource language handling, BIG may use vetted third-party large language models or machine translation technologies where permitted by contract and security requirements.

For public-sector and regulated environments, BIG can configure workflows to avoid the use of public or unsecured AI tools and can restrict processing to approved, controlled, and secure systems. Customer



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



data is not used to train or fine-tune AI models unless explicitly authorized in writing by the client. This approach supports the RFP's requirement that offerors disclose AI data practices and prohibit the use of agency data for AI model training without explicit consent.

For live interpretation, BIG's architecture may include self-hosted or controlled automatic speech recognition, in-house machine translation resources, configurable text-to-speech options, and secure integration layers. Where third-party components are used, they are evaluated for security, performance, reliability, and contractual suitability.

- [How your system handles domain-specific government and municipal terminology](#)

Our models are trained using domain- and client-specific translation memories (TMs) derived from historical human translations and post-editing by subject-matter experts. These curated datasets ensure that government and municipal terminology is accurately represented and consistently applied. During training, the models learn to replicate these domain-specific linguistic patterns, resulting in terminology alignment with client standards and regulatory language.

For live interpretation:

1. ASR keyterm biasing for proper nouns/acronyms,
2. custom NMT models trained on TM,
3. per-term IPA pronunciation overrides via SSML in TTS.

- [Quality assurance and accuracy measurement methodology \(e.g., BLEU scores, human evaluation, post-editing analysis\)](#)

BIG measures translation and interpretation quality through a combination of automated metrics, human evaluation, post-editing analysis, client feedback, and ongoing performance monitoring. We do not rely on a single metric because language quality depends on content type, audience, domain, risk level, and communication channel.

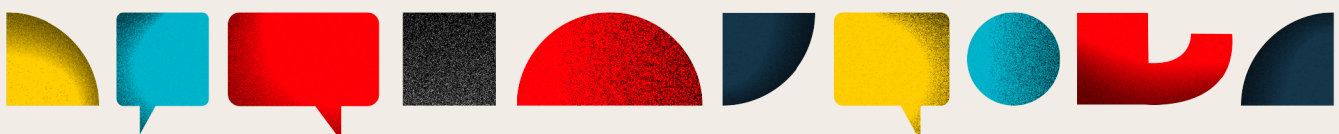
For written translation, BIG's quality methodology may include:

- BLEU, COMET, or other automated scoring where reference data is available.
- Quality estimation to identify high-risk or low-confidence segments.
- Human review for fluency, adequacy, terminology, accuracy, readability, cultural appropriateness, and formatting.
- Post-editing distance analysis to evaluate how much human correction was required.
- Terminology compliance checks against approved glossaries.
- Translation memory leverage analysis.
- Client feedback loops and corrective action tracking.



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



- Final QA checks prior to delivery.

For live interpretation and real-time AI-assisted workflows, BIG monitors performance using indicators such as:

- Automatic speech recognition confidence scores.
- Word error rate where measurable.
- Latency by workflow stage.
- Session stability and connectivity.
- Language channel performance.
- Transcript review, where available and authorized.
- Optional post-event linguist review for high-stakes meetings or public-facing sessions.

When AI confidence is low, content is sensitive, or accuracy risk is elevated, BIG can route work to human linguists, apply additional review, or recommend human interpretation or human translation instead of AI-only delivery. This allows public agencies to use AI appropriately while maintaining safeguards for legal, healthcare, public safety, benefits, emergency, and other high-impact communications.

- [How the platform is updated and improved over time](#)

Our platform follows a continuous improvement cycle driven by both data and performance monitoring. Models are regularly evaluated based on (a) growth in available training data and (b) the extent of post-editing required. When predefined thresholds are exceeded, models are retrained using updated translation memories and datasets. In parallel, we iteratively enhance our software architecture and machine learning methodologies to incorporate new features, improve scalability, and adopt state-of-the-art advancements.

For live interpretation, improvement efforts may include enhancements to segmentation, endpointing, latency reduction, glossary handling, speaker environment recommendations, language-channel performance, and integration stability.

This governance-based approach gives public agencies the benefits of evolving AI technology without exposing them to uncontrolled model behavior or unmanaged workflow changes.

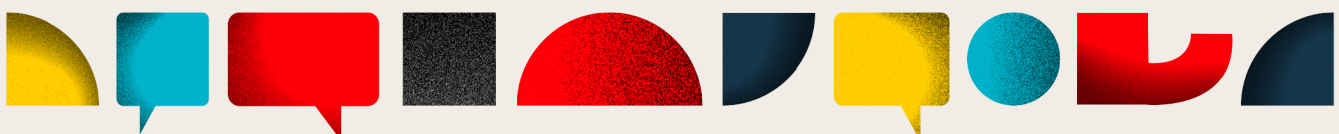
- [Known limitations in specific language pairs or content types and how they are addressed](#)

BIG is transparent about the limitations of AI-driven language technology. AI translation and interpretation can produce errors, especially in low-resource languages, complex legal or medical content, emergency



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



communications, idiomatic speech, overlapping speakers, poor audio quality, heavy accents, or terminology-dense material.

Rather than treating AI as a one-size-fits-all solution, BIG applies a risk-based service model.

Known limitations and mitigation strategies include:

- **Low-resource languages:** AI-only output may be less reliable for certain languages with limited training data. BIG mitigates this through human review, quality estimation, linguist escalation, and human-first workflows where appropriate.
- **High-stakes content:** Legal, medical, public safety, benefits, emergency, and regulatory content may require human review or human translation. BIG can default these content types to human linguist review.
- **Live meeting complexity:** Background noise, overlapping speakers, rapid exchanges, or unclear audio can reduce ASR accuracy. BIG mitigates this through pre-session planning, audio best practices, terminology preparation, captions/transcripts where appropriate, and human interpreter escalation options.
- **Names, acronyms, and local terminology:** Proper nouns and agency-specific terms may require configuration. BIG mitigates this through glossaries, key-term biasing, pronunciation guidance, and pre-event preparation.
- **AI confidence variability:** Where confidence thresholds are low, BIG can route content for review or prompt escalation to a human interpreter or linguist.

For languages such as Tigrinya, Hmong, Amharic, Khmer, Somali, Haitian Creole, and other low-resource or high-variability language pairs, BIG does not recommend unsupervised AI-only workflows for high-stakes content. Human review, human interpretation, or hybrid workflows are recommended based on the use case.

Language Coverage

Provide a complete list of languages supported for each service type (live voice, document translation, OPI/VRI). For each language, indicate: See a complete list of languages attached.

BIG Language Solutions supports language access services across multiple delivery modalities, including live voice interpretation and on-demand OPI/VRI, in over 300 languages and dialects. For the purposes of this response, the primary languages relevant to this engagement include: **Spanish, Mandarin, Cantonese, Vietnamese, Portuguese, Arabic, Russian, Haitian Creole, Somali, Korean, Tagalog, Polish, French, Hindi, Japanese, Gujarati, and Tigrinya.**

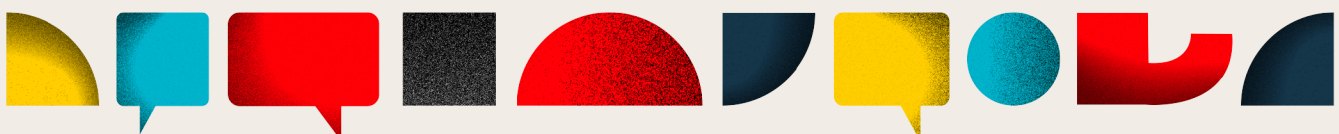
- [Availability for live voice interpretation](#)

BIG supports live voice interpretation in the primary languages listed above through qualified human



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



interpreters. Spanish is supported 24/7, with additional languages supported in alignment with operational coverage requirements and service design.

For AI-based live voice interpretation we support: Spanish, Mandarin, Cantonese, Vietnamese, Portuguese, Arabic, Russian, Korean, Tagalog, Polish, French, Hindi, Japanese, Gujarati.

- [Availability for on-demand OPI/VRI](#)

BIG supports on-demand OPI/VRI across the same primary languages through qualified human interpreters delivered via its remote interpretation platform.

- Human interpretation: 300+ languages and dialects

- [Availability for document translation](#)

BIG supports document translation across the same primary languages through machine and qualified human translators.

- Human translation: 300+ languages and dialects

- [Quality tier or confidence level \(e.g., human-reviewed vs. AI-only\)](#)

We can provide multiple indicators to reflect quality and confidence, depending on the use case. For translation, we offer a Quality Estimation score that predicts how accurate and reliable a given translation is, even without human review. Based on a client's risk tolerance, we can also deliver raw MT output for lower-risk scenarios, or apply stricter quality thresholds where needed. For live interpretation, we provide confidence scores from the ASR system. If confidence falls below a defined threshold, users can be prompted to switch to a human interpreter, ensuring continuity and reliability in more critical situations.

- [Any languages where AI-only output is not recommended and human review is required](#)

For AI Interpreter for Meetings or AI Interpreter for Conversations, a human review is not possible. Here, there is a possibility of switching to a human interpreter upon user request.

Government and Municipal Experience

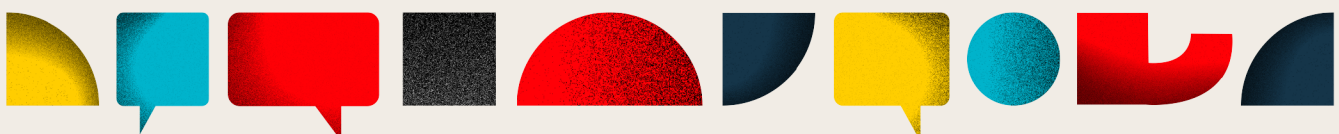
Describe your experience providing translation and language access services to government entities. Provide a minimum of five (5) government contracts performed within the past seven (7) years. For each, describe:

- Agency name, contact, and phone number
- Contract value and duration



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



- Types of services provided (live meetings, document translation, OPI, platform license)
- Volume of translations and interpretations performed
- Any cooperative purchasing contract experience (GSA Schedule, state contracts, GPOs)

Government Contracts #1

- Agency Name: Washington State Department of Health and Social Services (DSHS)
- Contact Person: Amanda Wilson, Mandy Wilson
- Phone Number: (425) 339-4051, (564)-669-3321
- Email Address: amanda.wilson3@dshs.wa.gov
- Contract value and duration: \$13.5 million, 5 years; Final term ends 2031 We have been servicing DSHS for various language services since 1995.
- Types of services provided: OPI, In the process of adding VRI
- Volume of interpretations performed: 450,000 minutes per month
- Any cooperative purchasing contract experience: Extensive

Government Contracts #2

- Agency Name: Colorado Parks and Wildlife
- Contact Person: Mark Koenig
- Phone Number: (303) 291-7612
- Email Address: mark.koenig@state.co.us
- Contract value and duration: Current estimated value is \$33,000 over two years, for Mark's agency only
- Types of services provided: Document Translation
- Volume of translations performed: Average of 3-5 requests per month
- Any cooperative purchasing contract experience: This account purchases from a cooperative agreement, NASPO

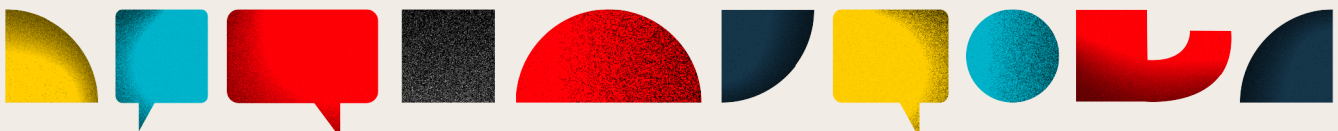
Government Contracts #3

- Agency Name: LA County Registrar Recorder & County Clerk
- Contact Person: Joy Xu
- Phone Number: (323) 643-2254
- Email Address: jxu@isd.lacounty.gov
- Contract value and duration: Estimated value for written translation is \$14 million with duration from 2019 to present
- Types of services provided: Document Translation and Print/Mail Services
- Volume of translations performed: Average of 400k-500k words per year into 18-23 languages
- Any cooperative purchasing contract experience: This contract is for election specific work, but pricing may be used by other County entities if approved.



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



Government Contracts #4

- Agency Name: State of Colorado
- Contact Person: Amy Risley
- Phone Number: (303) 866-5663
- Email Address: amy.risley@state.co.us
- Contract value and duration: \$500K a year and 5 years through NASPO; Final term ends 2030
- Types of services provided: OPI, VRI
- Volume of interpretations performed: 900K minutes per year
- Any cooperative purchasing contract experience: This is a NASPO contract

Government Contracts #5

- Agency Name: State of Nevada
- Contact Person: Miriam Garcia
- Phone Number: (775) 531-3307
- Email Address: miriam.garcia@admin.nv.gov
- Contract value and duration: 4 years on current contract, but have been on previous contracts since 2019. Estimate value of current contract is NTE \$500,000
- Types of services provided: Document Translation and OPI, VRI
- Volume of translations and interpretations performed: 2-3 written translation requests per week currently. Interpretation volume is 900K minutes per year
- Any cooperative purchasing contract experience: All state of Nevada entities may purchase from this contract including the University and Community College System, the Court System, the Legislative Counsel Bureau, and Political Subdivisions (i.e., cities, counties, school districts, etc.)

Geographic Coverage and Scalability

Describe your company's ability to provide services nationally. Identify any limitations on service delivery by geography, time zone, or language availability. Describe your capacity to scale services during high-demand periods such as election cycles, emergency events, or major municipal initiatives.

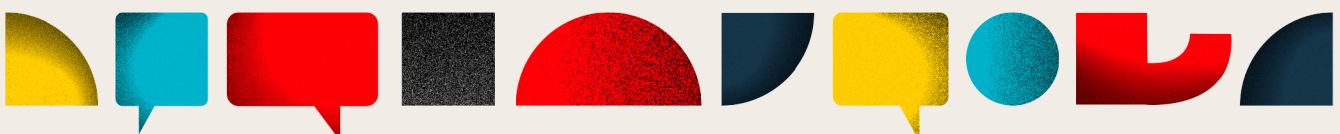
BIG Language Solutions has the national reach, global infrastructure, and operational depth required to support participating public agencies across the United States, regardless of geography, time zone, agency size, or language need.

We operate through a globally distributed service delivery model designed for resilience, scalability, and uninterrupted coverage. Our primary Centers of Excellence are located in the United States and India, enabling 24/7/365 support across multiple time zones. In addition, BIG maintains six offices worldwide and a broad



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



network of professional linguists, interpreters, project managers, quality reviewers, and support teams located throughout North America, Latin America, Europe, and Asia.

This distributed model allows us to balance workloads across regions, maintain redundancy for critical languages, and continue service delivery during regional disruptions, emergencies, weather events, or unexpected spikes in demand. For public agencies, this means reliable access to multilingual communication support during both routine operations and urgent situations.

BIG does not have geographic limitations on service delivery within the United States. We are equipped to support municipalities, counties, state agencies, educational institutions, healthcare entities, social service agencies, and other public-sector organizations nationwide. Services can be delivered remotely, virtually, by phone, through secure portals, and through integrated workflows. Where onsite or locally informed support is required, we can draw from our national linguist network and targeted recruiting capabilities.

Capacity to scale services during high-demand periods

BIG has extensive experience supporting high-volume, time-sensitive, and mission-critical language access needs for public-sector and regulated clients. We understand that public agencies may experience sudden surges in demand during election cycles, public health events, natural disasters, emergency response efforts, benefits enrollment periods, community outreach campaigns, major municipal initiatives, and other high-visibility public communications.

Our scalability model combines experienced operations leadership, technology-enabled workflows, a large, vetted linguist network, and flexible resource allocation. This allows us to rapidly adjust staffing, production assignments, and workflow priorities without sacrificing quality, security, or responsiveness.

For translation projects, BIG begins by assessing the scope, language mix, file types, subject matter, urgency, formatting needs, and quality requirements. Work is then assigned strategically across experienced project managers, production teams, linguists, editors, and quality reviewers based on language, content type, volume, and subject-matter expertise. This structure allows us to manage large document sets, urgent public notices, emergency communications, multilingual outreach campaigns, and recurring agency materials efficiently and consistently.

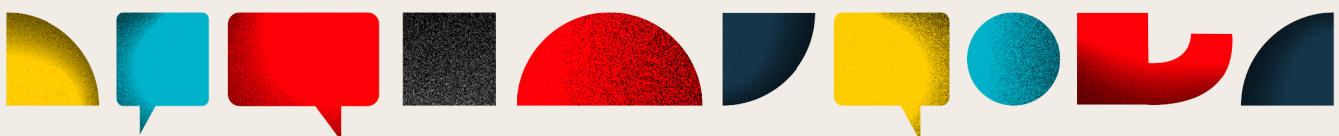
BIG maintains a trusted network of more than 7,500 linguists, many of whom work with us regularly. This gives us the ability to respond quickly to increased demand across common, emerging, and lower-incidence languages. When additional resources are needed, our Language Request process supports 24/7 recruiting, profiling, vetting, and onboarding of qualified professionals.

For interpretation, BIG maintains broad coverage for over-the-phone, video remote, and onsite interpretation needs. We actively recruit from local communities to strengthen coverage in hard-to-fill and low-resource languages, helping ensure that our interpreter network reflects the communities public agencies serve. Our Vendor Management Office is dedicated to identifying, recruiting, credentialing, and monitoring interpreters through multiple channels, including direct community outreach.



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



Our approach is especially valuable for municipalities and public agencies serving diverse populations, rural communities, refugee and immigrant populations, and regions with changing language access needs. Beyond language proficiency, we prioritize interpreters and linguists who demonstrate cultural awareness, professionalism, confidentiality, empathy, and experience in public-sector or regulated environments.

Through this proven model, we can scale quickly while maintaining quality, consistency, and compliance. Whether supporting routine agency operations, a large multilingual document initiative, a surge in OPI/VRI demand, an election-related communication campaign, or an emergency public safety event, we have the infrastructure, personnel, and experience to deliver reliable language access nationwide.

References and Past Performance

Provide a minimum of three (3) public agency references for translation and/or language access service contracts completed within the past five (5) years. References must be from government clients. For each reference, provide:

- Agency name
- Contact name, title, phone number, and email address
- Contract value and duration
- Types of services provided
- Volume of translations/interpretations performed
- Languages supported

Reference #1

- Agency Name: Prince George's County Public Schools
- Contact Name: Jennifer Love
- Title: Supervisor, Language Access & Engagement
- Phone Number: (301)-408-5511
- Email Address: jennifer.love@pgcps.org
- Contract value and duration: \$500K a year, 15 years
- Types of services provided: OPI
- Volume of translations/interpretations performed: 750,000 minutes per month
- Languages supported: All the primary languages

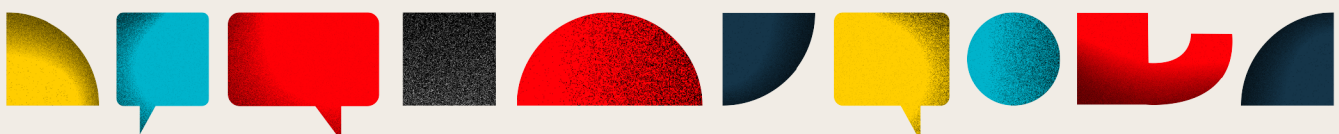
Reference #2

- Agency Name: New York Dept. of Agriculture & Markets
- Contact Name: Mark Lansing
- Title: Director of Human Resources
- Phone Number: (518) 457-8851



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



- Email Address: Mark.Lansing@agriculture.ny.gov
- Contract value and duration: Partnered with Mark Lansing specifically since 2020, with an estimated value of \$60,000 to date.
- Types of services provided: Document Translation
- Volume of translations/interpretations performed: 2-3 written translation requests per month
- Languages supported: NY Top 12 Spanish (United States), Chinese (Traditional and Simplified), Russian, Yiddish, Bangla (Bangladesh), Korean, Haitian Creole, Italian, Arabic, Polish, French (West Africa), Urdu, and more

Reference #3

- Agency name: Washington State Department of Labor & Industries
- Contact name: Tiffany Richard
- Title: Bilingual Communication Consultant, Language Access Program
- Phone number: (360) 902-6799
- Email address: riti235@LNI.WA.GOV
- Contract value and duration: Partnered with Tiffany since 2022, with the L&I department since 2004. The current average annual written translation value is \$750,000.
- Types of services provided: Document Translation
- Volume of translations/interpretations performed: We facilitate an average of 65-80 written translation requests per day.
- Languages supported: Any language requested, including those of lesser diffusion.

EVALUATION SECTION 2: AI TECHNOLOGY CAPABILITY, LANGUAGE COVERAGE & ACCURACY

Accuracy and Quality Standards

Offerors must demonstrate measurable translation and interpretation accuracy. Address the following:

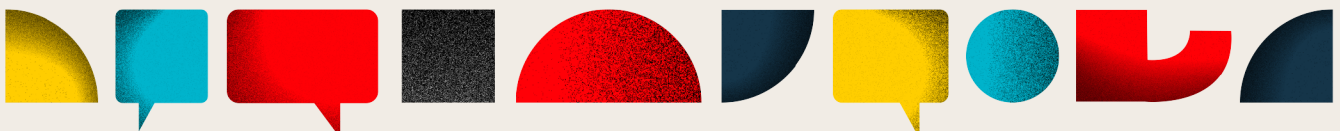
- [Published or internally measured accuracy rates by language pair and content type](#)

Accuracy benchmarks are established for each language using a combination of BLEU scores, human evaluation, and terminology compliance checks. Translations are compared against reference corpora, with linguists reviewing a sample of outputs for grammar, meaning, and cultural appropriateness. Benchmarks are updated regularly to reflect improvements and maintain consistency across languages.



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



- [Methodology used to measure translation quality \(automated metrics, human evaluation, customer feedback\)](#)

BIG ensures translation accuracy through a certification-driven quality framework supported by external audits, rigorous linguist vetting, and continuous monitoring.

BIG maintains ISO 17100 and ISO 9001:2015 certifications, which serve as the cornerstones of our quality process. ISO 17100, specific to the translation industry, validates our end-to-end workflow, from linguist qualifications to project management and delivery, through independent external audits. ISO 9001 requires an annual audit of our Quality Management System, including hiring practices, linguist performance measurement, and our corrective (CAR) and preventive (PAR) action processes.

Translation accuracy is further ensured through a comprehensive service delivery structure:

- **Linguist vetting and certification:** Only linguists with proven expertise, advanced academic credentials, and industry experience are selected.
- **Ongoing training:** All linguists are trained on BIG's proprietary tools and receive continuous development tailored to client and project needs.
- **Quality monitoring:** Accuracy, style, and cultural appropriateness are reviewed at multiple stages, with feedback loops to strengthen consistency over time.

Through this structured and externally validated process, BIG consistently delivers translations that are precise, accurate, and both culturally and linguistically appropriate, ensuring the highest level of quality in every engagement.

- [How quality assurance is performed prior to delivery for document translations](#)

All translations pass through layered quality assurance checks before delivery. Objective errors are corrected immediately at no charge, while subjective changes (such as style or terminology preferences) are implemented upon request. Updates are captured in translation memories and glossaries to ensure future consistency.

This structured approach ensures that every deliverable meets the highest standards of accuracy, cultural relevance, and compliance, with measurable quality on a scale.

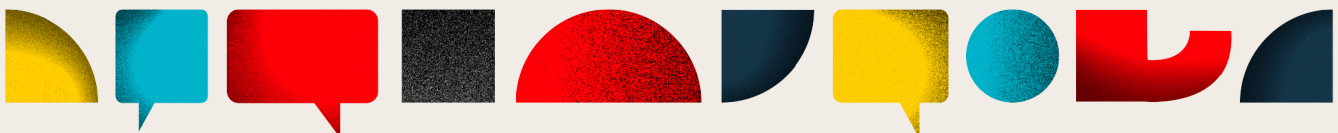
- [Real-time quality monitoring for live interpretation services](#)

BIG Language Solutions employs a robust real-time quality monitoring framework to ensure the highest standards of accuracy, professionalism, and compliance during live interpretation sessions. This



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



approach combines trained linguistic quality assurance personnel with advanced monitoring tools to continuously evaluate performance as sessions occur.

Designated quality monitors may observe sessions in real time to assess key performance indicators, including accuracy, completeness, terminology adherence, interpreter conduct, and compliance with client-specific protocols (e.g., HIPAA, confidentiality, neutrality). Where appropriate, secure communication channels enable discreet, real-time feedback to interpreters to address minor issues without disrupting the session.

In critical scenarios, escalation protocols allow for immediate intervention, including interpreter replacement if necessary, ensuring continuity of service and minimizing risk to end users.

Additionally, BIG leverages technology-enabled monitoring capabilities, including call analytics and AI-assisted tools (where permitted), to identify potential quality risks such as omissions, latency issues, or terminology inconsistencies.

All monitored sessions are documented, and insights are incorporated into ongoing performance management, training, and continuous improvement programs.

This real-time monitoring capability ensures consistent delivery of high-quality, compliant interpretation services.

- [Human review and post-editing capabilities and workflows](#)

BIG Language Solutions maintains comprehensive human review and post-editing workflows to ensure the accuracy, quality, and contextual appropriateness of all translated content, including outputs generated through machine translation (MT) or AI-assisted tools.

All linguists engaged in post-editing are qualified professionals with subject-matter expertise and are trained in both light post-editing (LPE) and full post-editing (FPE) methodologies, depending on client requirements and content sensitivity.

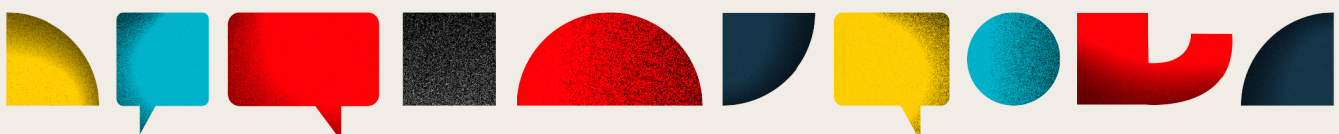
Our standard workflow includes:

- Initial translation (human or MT-assisted, as approved)
- Structured human review and post-editing by a second linguist
- Terminology validation against approved glossaries and style guides
- Quality assurance checks for accuracy, fluency, consistency, and compliance
- Final review prior to delivery



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



For sensitive content (e.g., healthcare, legal, government), we implement full human review workflows, ensuring that all deliverables meet strict quality and regulatory standards, including HIPAA compliance where applicable.

We also leverage technology-enabled QA tools (e.g., terminology management systems, automated QA checks) to support linguists, while ensuring that final quality responsibility remains with human reviewers.

All workflows are configurable based on client needs, with options for human-only translation, MTPE (Machine Translation Post-Editing), and multi-step review processes.

This structured, human-centric approach ensures high-quality, reliable, and contextually accurate language services across all engagements.

- [Escalation paths when AI confidence is low or content is flagged as high-stakes](#)

BIG has established structured escalation protocols to ensure quality, accuracy, and compliance when AI-assisted outputs fall below confidence thresholds or when content is identified as high-stakes.

Our workflows incorporate automated and manual triggers to flag:

- Low-confidence machine translation outputs
- Terminology inconsistencies or ambiguities
- Sensitive or regulated content (e.g., healthcare, legal, government)
- Potential compliance risks (e.g., HIPAA, confidentiality requirements)

When such conditions are detected, the following escalation steps are applied:

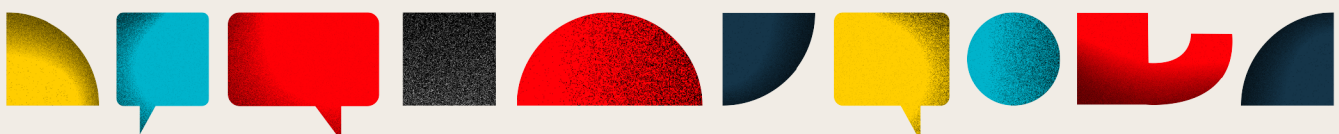
1. **Automatic Routing to Human Linguists**
Flagged content is immediately routed to qualified linguists for full human review or re-translation, bypassing automated workflows.
2. **Enhanced Review Protocols**
A multi-tier review process is initiated, including subject-matter expert (SME) validation where required.
3. **Quality Assurance Oversight**
Senior QA reviewers assess flagged segments for accuracy, completeness, and adherence to terminology and client-specific guidelines.
4. **Audit Logging and Continuous Improvement**
All escalations are logged and analyzed to refine AI models, improve confidence thresholds, and prevent recurrence.

For high-stakes use cases, BIG defaults to human-first or human-only workflows, ensuring that AI is used only where appropriate and with full oversight.



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



These escalation mechanisms ensure that risk is proactively managed and that all deliverables meet the highest standards of quality and compliance.

Real-Time Interpretation Performance

For Workstream 1 (Live Voice Interpretation), provide the following performance benchmarks:

PERFORMANCE METRIC	OFFEROR'S COMMITTED SLA
AI interpretation latency (audio-to-output delay)	__10__ seconds
Platform uptime guarantee	__99.9__ %
Support for concurrent language channels per session	__5__ simultaneous languages
Maximum concurrent meeting participants supported	__50__ (solution upgrade for additional participants in development)
Connectivity recovery time (if session drops)	__30__ seconds

EVALUATION SECTION 3: SECURITY, COMPLIANCE & DATA PRIVACY

Security Certifications

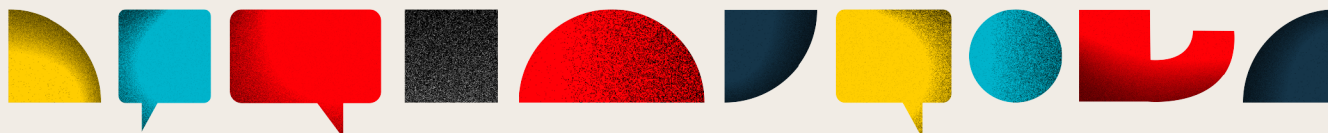
Provide documentation of all current security certifications and audits. At minimum, Offerors must provide:

- Current SOC 2 Type II audit report (or equivalent): See attached
- ISO 27001 certification (if applicable): See attached
- FedRAMP authorization documentation (if applicable): Not Applicable
- CJIS compliance documentation (if services are proposed for law enforcement use): Not Applicable



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



- [HIPAA BAA template \(required if services may process PHI\)](#): See attached

Data Handling Practice

[Describe your organization's data handling practices for municipal client data, including:](#)

BIG maintains rigorous data handling practices to ensure the security, confidentiality, and integrity of all municipal client data. Our approach aligns with applicable federal, state, and local regulations, as well as industry best practices for data protection.

We collect and process only the minimum data necessary to perform contracted services. All data is used strictly for authorized purposes and in accordance with client agreements.

We treat municipal data with the highest level of care, security, and accountability. Our data handling practices are built around a security-first, least privilege model, ensuring that sensitive information is protected at every stage of the workflow.

Key highlights:

- End-to-end encryption and secure infrastructure
- Strict access controls with role-based permissions
- No use of unsecured or public AI/MT tools for sensitive data
- Trained, vetted linguists bound by confidentiality agreements
- Defined data retention and secure deletion policies
- Rapid incident response and transparent reporting

We align our practices with government expectations and industry standards, enabling municipalities to confidently rely on our services for secure, compliant language support, resulting in the trusted handling of public-sector data with zero compromise on security or compliance.

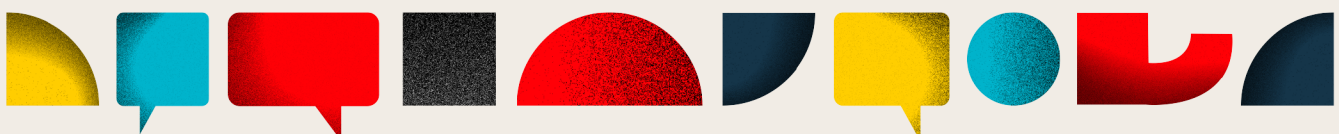
- [What data is collected, stored, and processed during translation/interpretation sessions](#)

BIG Language Solutions collects only the minimum data necessary to deliver language services. This typically includes client-provided content (documents, audio, or video), live session data (audio/video streams and basic session details such as date, time, and language pair), limited participant identifiers (e.g., name or role, if required), and the resulting translated or interpreted output. Additionally, system-generated data such as access logs and basic performance metrics may be collected to support service



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



delivery and quality assurance. Optional elements—such as session recordings or AI-assisted processing—are used only with explicit client authorization. All data is handled in accordance with strict confidentiality, security, and data minimization principles.

- [Data retention schedule and deletion processes](#)

Our standard data retention policy maintains records only as long as necessary for contractual, regulatory, or legal purposes, after which data is securely deleted or anonymized. Retention periods can be customized by client, with options to shorten, extend, or apply different rules by data type (e.g., recordings, transcripts, metadata). Policies are enforced through automated retention schedules, with audit trails to verify compliance.

Secure data deletion is performed using industry-standard wiping and cryptographic erasure methods, with confirmation logs maintained. For right-to-be-forgotten requests, all identifiers are removed from active systems, backups, and archives within defined timelines, ensuring data cannot be reconstructed. Completion is documented and auditable for compliance.

- [Whether customer data is used to train or fine-tune AI models \(must disclose and allow opt-out\)](#)

No, customer data is not used to train or fine-tune our AI models. All data is processed solely for the requested service, and strict data segregation and confidentiality measures prevent its use in model development.

- [Geographic location of all data processing and storage \(U.S.-based preferred\)](#)

All data will be processed and stored in the U.S.

- [Sub-processor list and data sharing agreements](#)

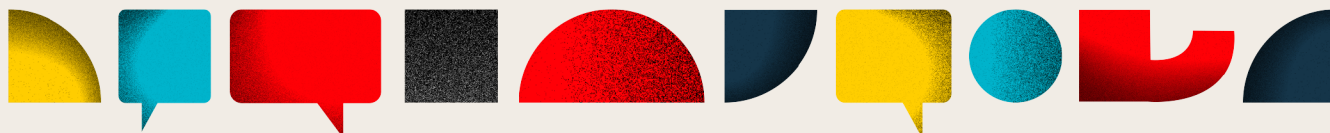
BIG Language Solutions maintains a transparent and controlled approach to the use of sub-processors in the delivery of language services. Sub-processors may include technology providers (e.g., secure hosting, translation management systems), communication platforms, and, where applicable, vetted linguists or subcontractors.

A current list of sub-processors is maintained and made available to clients upon request or as part of contractual documentation. This list includes the name, service provided, and geographic location of each sub-processor.



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



BIG enters into binding data processing agreements (DPAs) or equivalent contractual arrangements with all sub-processors to ensure:

- Confidentiality and non-disclosure obligations
- Compliance with applicable data protection laws and regulations
- Implementation of appropriate administrative, technical, and physical safeguards
- Restrictions on further data sharing without authorization

Sub-processors are granted access only to the minimum data necessary to perform their designated functions, in accordance with the principle of least privilege.

- **Breach notification process and timeline (must be within 72 hours of discovery)**

Breach notifications are managed in accordance with applicable local and international privacy laws, including the requirement to notify relevant authorities and impacted clients within 72 hours of discovery where legally required. We promptly identify affected jurisdictions, coordinate with legal and compliance teams, and ensure all notifications are issued within mandated timelines, with the required content and supporting documentation.

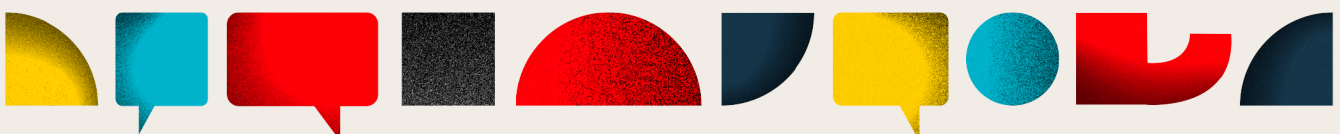
During a security incident, we provide full investigative support, including access to logs, audit trails, system records, and relevant documentation. We assist with root cause analysis, regulatory reporting, client communications, and remediation activities to ensure a timely, compliant, and transparent resolution process.

Upon identification of a security incident, our incident response procedures are immediately activated. System logs are reviewed, a full audit investigation is conducted, and findings are documented in a formal incident report. Impacted parties are notified without undue delay and, where applicable, within the required 72-hour timeframe. Remediation and containment measures are communicated throughout the process to ensure transparency, risk mitigation, and resolution.



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



EVALUATION SECTION 4: IMPLEMENTATION, ONBOARDING & SUPPORT

Implementation Plan

Describe your standard implementation process for a new municipal client. Address the following:

BIG Language Solutions follows a structured, phased implementation approach to ensure a smooth, secure, and efficient onboarding of municipal clients. Most implementations are completed within 4–6 weeks of contract execution, with the ability to adjust based on the client's goals. Our approach is structured in four phases:

- **Phase 1: Planning**

We collaborate with customer operational and technical stakeholders to align priorities, timelines, and success measures. This includes technical calibrations for call centers, IT security reviews, and device planning. Project and communication plans are established, and tailored dashboards for SLAs, financial tracking, quality, and compliance are configured.

- **Phase 2: Deployment**

Our field technicians deploy equipment onsite and conduct staff training with minimal disruption. Technical integrations (call centers) are tested and validated, and customers receive training on our management platforms LanguageVault®, InterpVault™, our solutions, and reporting processes to build internal expertise.

- **Phase 3: Optimization & Support**

In the first quarter post-deployment, we meet with stakeholders bi-weekly or monthly to optimize workflows, interfaces, and support.

- **Phase 4: Sustainment**

We hold quarterly business reviews covering SLA performance, metrics, technical advancements, and best practices to ensure long-term success.

This structured approach ensures minimal disruption, rapid adoption, and consistent delivery of high-quality language services for municipal clients.

- Typical time from contract execution to full deployment (target: under 30 days for cloud deployments)

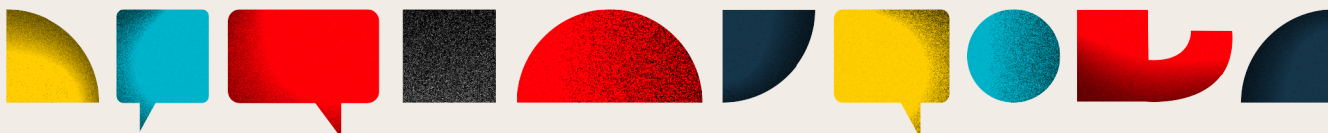
Most implementations are completed within 2–6 weeks of contract execution, depending on the solution/s and level of customization required, with the ability to adjust based on the client's goals.

- Technical requirements on the agency side (hardware, software, network)



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



BIG Language Solutions is committed to minimizing technical burden on municipal clients. Our language services are designed to operate with standard, widely available infrastructure. Getting started with our services is simple—no complex setup required.

No specialized hardware or heavy software installations are needed for 'out-of-the-box' solutions. Our platforms are secure, browser-based, and designed to work within standard municipal IT environments, resulting in fast deployment with minimal IT effort and zero disruption.

- [Integration support for common government platforms \(Granicus, Civic Plus, Tyler Technologies, Accela, NeoGov, etc.\)](#)

We are API-enabled and can integrate with common government platforms. Our development team works directly with client IT teams to design and implement integrations as needed, ensuring seamless compatibility with existing environments.

This flexibility allows us to support virtually any platform, embedding interpretation and translation services directly into existing workflows while maintaining secure, compliant, and reliable performance

- [Data migration and historical translation import capabilities](#)

BIG Language Solutions provides structured and secure data migration services to support the onboarding of new clients, including the import of historical translation assets and legacy data. We make sure nothing valuable is lost when you switch providers.

Our team securely migrates and integrates your existing translation memories, glossaries, and historical content into our systems—so you can continue where you left off.

Key capabilities:

- Import of TM, glossary, and legacy translation files
- Data cleansing and quality improvement
- Secure transfer and controlled access
- Optimization for faster, more consistent future translations
- Full client ownership and easy export at any time

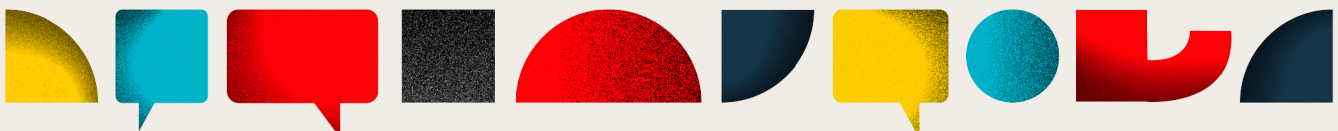
This results in better consistency, reduced costs, and faster turnaround from day one.

- [Customization and configuration process \(terminology glossaries, branding, user roles\)](#)



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



BIG Language Solutions provides a structured and flexible customization process to align language services with each municipal client's operational, linguistic, and branding requirements. We configure our services to match how you work—not the other way around.

From day one, we customize:

- **Terminology** – Your glossaries are integrated to ensure consistent, accurate language
- **Brand Voice** – We align with your tone, style, and public communication standards
- **User Roles** – Access and permissions are configured to fit your teams and workflows

We also set up approval workflows, routing rules, and reporting to mirror your internal processes, resulting in language services that feel like a seamless extension of your organization—consistent, secure, and easy to manage.

Training and Support

Describe the training and ongoing support provided to agency staff:

- [Initial administrator and end-user training \(virtual and/or on-site options\)](#)

BIG provides initial training for both administrators and end users during implementation. Administrator training focuses on account setup, user access, reporting, portal navigation, service workflows, escalation procedures, and account management. End-user training focuses on the practical steps staff need to request services, initiate interpretation sessions, submit translation requests, work effectively with interpreters and translators, and access support when needed.

Training sessions can be scheduled by department, role, shift, or location to accommodate agency operations and reduce disruption to daily service delivery. For public agencies with multiple departments or user groups, BIG can provide targeted training for teams such as customer service, public health, social services, public safety, courts, education, housing, utilities, community outreach, and administrative offices.

- [Training materials: documentation, video tutorials, knowledge base](#)

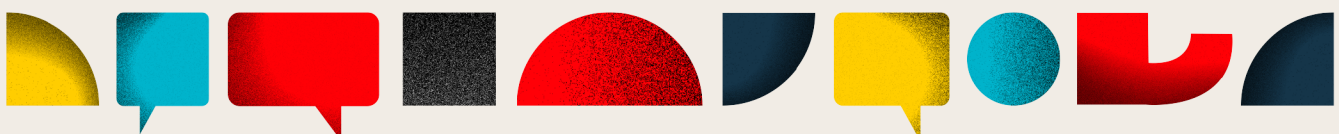
BIG provides easy-to-use training materials and reference resources to support ongoing adoption. These may include quick reference guides, user instructions, portal guides, workflow documents, FAQs, and other job aids tailored to the agency's services.

Clients can also view training documentation in the 'Support' menu of BIG's management portals:



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



InterpVault™ — BIG's interpretation portal, which provides visibility into interpretation usage, activity, reporting, invoices, and account information.

LanguageVault® — BIG's translation portal, which supports translation request management, project visibility, reporting, invoices, and account activity.

Quick reference guides are available for both interpretation and translation services, helping staff quickly understand how to access services, submit requests, review activity, and use available portal features.

- [Ongoing training for new staff and platform updates](#)

BIG's support does not end at go-live. We provide ongoing training and refresher support to help agencies onboard new staff, reinforce best practices, and adapt to platform updates or workflow changes.

During implementation, BIG conducts a contract kickoff and user training sessions covering topics such as how to initiate interpretation calls, submit translation requests, interact effectively with interpreters and translators, navigate InterpVault™ and LanguageVault®, access reports, and escalate questions or issues.

Training continues through go-live and early stabilization. BIG's Client Relations team, technical support staff, and account management team remain available for refresher sessions, staff huddles, one-on-one support, and additional department-level training as needed. This ensures that agencies can maintain consistent service adoption even as staffing, language needs, or internal workflows change.

- [Technical support tiers \(Tier 1/2/3\) and escalation procedures](#)

BIG provides structured technical support with clear escalation paths to ensure issues are addressed quickly and appropriately. Support is organized by severity and complexity:

- **Tier 1:** Issues are handled directly.
- **Tier 2:** Issues are escalated into our ticketing system with an eight-hour response target.
- **Tier 3:** Issues receive a two-hour response target.

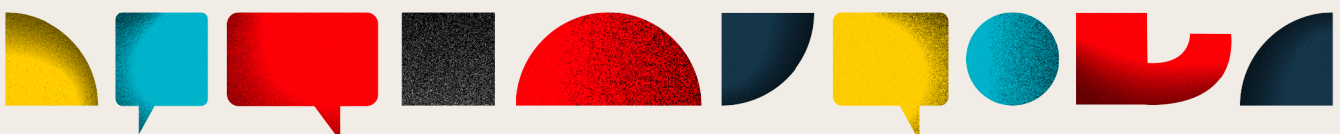
All concerns and complaints are handled by our Account Management team under our Customer Feedback SLA, which includes a 24-hour response and 72-hour resolution goal. Issues are logged, investigated, and followed through to closure, with findings and preventive measures documented.

Your dedicated account manager will be available for ongoing reviews, optimization, and escalation management.



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



- **Dedicated account management and customer success support**

BIG assigns each agency a dedicated account manager who serves as the primary point of contact from onboarding through ongoing service delivery. This account manager coordinates implementation, monitors service performance, supports issue resolution, and works closely with agency stakeholders to ensure BIG's services continue to align with operational needs, usage patterns, and language access goals.

To support long-term success, BIG schedules regular check-ins and quarterly business reviews to review service utilization, reporting, quality trends, SLA performance, upcoming needs, and opportunities for improvement. These meetings allow BIG to proactively adapt workflows, training, staffing, and support as agency needs evolve. Our customer success approach is designed to provide responsive day-to-day support while also helping agencies continuously strengthen their language access programs.

- **Support hours and response time SLAs by ticket priority**

BIG provides toll-free technical support 24/7/365 to ensure agencies have access to assistance whenever services are needed, including after hours, weekends, holidays, and during urgent or high-demand events.

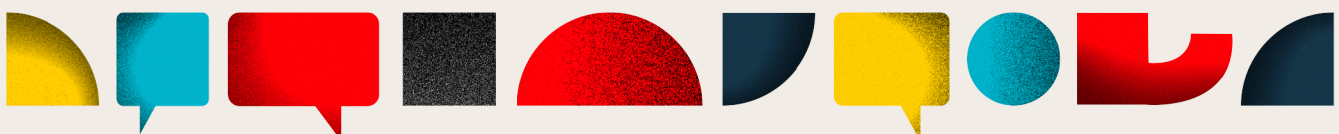
When an issue is reported, BIG's support team works directly with the end user to quickly diagnose the issue, determine severity, and either resolve it immediately or route it through the appropriate escalation path. Issues are tracked through our ticketing process to ensure visibility, accountability, and follow-through to closure.

Ticket Priority	Description	Response Target
Level 1	Routine questions or issues that can be resolved directly by support staff	Handled immediately at the first point of contact
Level 2	Issues requiring additional troubleshooting, coordination, or ticket escalation	8-hour response target
Level 3	Urgent or complex technical or operational issues requiring advanced support	2-hour response target



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



For reported concerns and service issues, BIG follows a 24-hour response and 72-hour resolution SLA. Your dedicated account manager will also remain available for ongoing reviews, service optimization, escalation management, and coordination with BIG's technical and operations teams as needed.

Service Level Agreements (SLAs)

Provide proposed SLAs for all service categories. At minimum, address:

- System uptime guarantee (minimum 99.9% required for Workstreams 1 and 3)

Noted, and agreed

- Document translation turnaround times by priority tier (standard, urgent, emergency)

Project Type	Word Volume	Standard Turnaround	Rush Turnaround
Standard human translation	Up to 2,000 words	1-3 business days	Rush turnaround times may be requested and would be confirmed on a case-by-case basis.
Standard human translation	2,001–10,000 words	3-7 business days	Same as above
Standard human translation	10,001+ words	2000 words per day	Same as above

- OPI/VRI average speed-to-connect targets by language

OPI: 20 seconds average across all languages

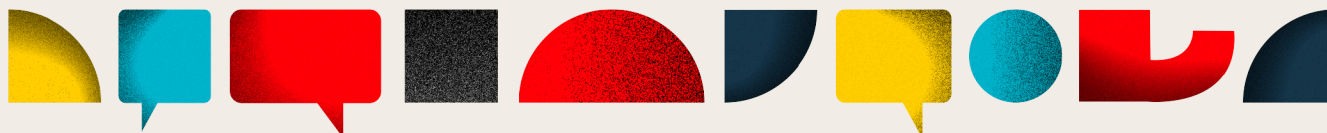
VRI: 14 seconds average across all languages

BIG can provide language-pair and content-type accuracy benchmarks upon request or during implementation based on the selected workflow, content domain, and quality tier.



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com



- [Customer support response time commitments by ticket severity](#)

BIG's technical support team works directly with end users to quickly assess each reported issue, determine the appropriate severity level, and begin resolution or escalation. Issues are handled through a structured support process to ensure timely response, clear ownership, and follow-through to closure.

Ticket Priority	Description	Response Target
Level 1	Routine questions or issues that can be resolved directly by support staff	Handled immediately at the first point of contact
Level 2	Issues requiring additional troubleshooting, coordination, or ticket escalation	8-hour response target
Level 3	Urgent or complex technical or operational issues requiring advanced support	2-hour response target

All escalated issues are documented in BIG's ticketing system, monitored through resolution, and reviewed as needed to identify corrective actions or opportunities for process improvement.

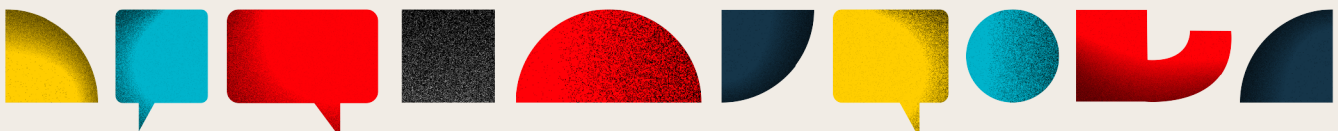
- [Planned maintenance windows and advance notification requirements](#)

Unless you need customized architecture, there is no maintenance required.



3414 Peachtree Road NE, Suite 465
Atlanta, GA 30326

+1 800.208.2620
info@biglanguage.com
biglanguage.com





CERTIFICATE

Certificate Registration No: 951 25 6383

The Certification Body of
TÜV SÜD AMERICA INC.

Certifies that the organization



BIG LANGUAGE SOLUTIONS, LLC

3424 Peachtree Rd NE, Suite 2060,
Atlanta, GA 30326 USA

for the scope

Applies to Web Translation, Document Translation, and Interpretation Services
Provided by All Our Entities—Language Link, DWL, Big IP, Protranslating, ISI, and
Law Linguists—Supported by Our IT, Administration, HR, Development and
Operations Functions

See attachment for complete listing of sites

has established and applies an Information Security Management System.
An audit was performed and has furnished proof that the requirements according to
“Statement of Applicability”

ISO/IEC 27001:2022

are fulfilled.

The certificate is valid from April 24, 2025 until April 23, 2028
With a re-issue date on N/A and Version of the Statement of Applicability:
Version-1.0 Date- 25-Oct-2024

Michael Fernald
Head of Central Certification Body
Page 1 of 2



TÜV SÜD America Inc • 401 Edgewater Place, Suite 500 • Wakefield, MA 01880 USA • www.TUVSUD.com

The validity of this certificate is contingent on the company maintaining its management system to the requirements
of the indicated standard and is subject to regular monitoring by TÜV SÜD America.



CERTIFICATE

Certificate Registration No: 951 25 6383

Certificate Holder:
BIG LANGUAGE SOLUTIONS, LLC
3424 Peachtree Rd NE, Suite 2060,
Atlanta, GA 30326 USA

At the Sites	Specific Scope Site
BIG LANGUAGE SOLUTIONS, LLC 3424 Peachtree Rd NE, Suite 2060, Atlanta, GA 30326 USA	Central Function -Applies to Web Translation, Document Translation, and Interpretation Services Provided by All Our Entities—Language Link, DWL, Big IP, Protranslating, ISI, and Law Linguists—Supported by Our IT, Administration, HR, Development and Operations Functions
BIG LANGUAGE SOLUTIONS INDIA PRIVATE LIMITED Skymark One, Tower E, 10th & 11th Floor, Sector 98, Noida, UP 201301 India	Applies to Web Translation, Document Translation, and Interpretation Services Provided by All Our Entities—Language Link, DWL, Big IP, Protranslating, ISI, and Law Linguists—Supported by Our IT, Administration, HR, Development and Operations Functions

Michael Fernald
Head of Central Certification Body
Page 2 of 2



TÜV SÜD America Inc • 401 Edgewater Place, Suite 500 • Wakefield, MA 01880 USA • www.TUVSUD.com

The validity of this certificate is contingent on the company maintaining its management system to the requirements of the indicated standard and is subject to regular monitoring by TÜV SÜD America.



SOC 2[®] TYPE 2 REPORT ON CONTROLS RELEVANT TO SECURITY FOR TRANSLATION APPLICATION SERVICES

BIG LANGUAGE SOLUTIONS, LLC

MARCH 1, 2024 TO FEBRUARY 28, 2025

BIG

LANGUAGE SOLUTIONS



BIG LANGUAGE SOLUTIONS, LLC

Table of Contents

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT.....	1
SECTION 2: MANAGEMENT'S ASSERTION.....	6
SECTION 3: DESCRIPTION OF THE SYSTEM.....	9
SCOPE OF REPORT AND DISCLOSURES	10
Overview	10
Trust Services Categories and Related Criteria	10
Scope	11
Sub-Service Organizations	12
Significant Changes during the Examination Period	12
Subsequent Events.....	12
System Incidents.....	12
Using the Work of the Internal Audit Function	12
OVERVIEW OF OPERATIONS AND THE SYSTEM	13
Company Overview and Background	13
Overview of the Translation Application Services System	13
Principal Service Commitments and System Requirements	13
OVERVIEW OF RELEVANT INFRASTRUCTURE.....	15
Infrastructure	15
Software	16
People	16
Procedures.....	16
Data.....	19
RELEVANT ASPECTS OF CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATIONS SYSTEMS, AND MONITORING	20
Control Environment	20
Risk Assessment	22
Information and Communication Systems.....	24
Monitoring	25
CATEGORIES, CRITERIA, AND RELATED CONTROLS	27
COMPLEMENTARY CONTROL CONSIDERATIONS	28
SECTION 4: CATEGORIES, CRITERIA, CONTROL DESCRIPTIONS, RELATED CONTROLS AND TESTS OF OPERATING EFFECTIVENESS	29
INFORMATION PROVIDED BY THE SERVICE AUDITOR	30
Introduction	30
Tests of Operating Effectiveness.....	30
Types of Tests Performed.....	31
Procedures for Assessing Completeness and Accuracy of IPE	31
Sampling Methodology	32
CATEGORIES, CRITERIA, AND RELATED CONTROLS	33
Security (Common Criteria to All Categories).....	33
SECTION 5: INFORMATION PROVIDED BY THE SERVICE ORGANIZATION THAT IS NOT COVERED BY THE SERVICE AUDITOR'S REPORT.....	83
Management's Responses to the Testing Exceptions.....	84

SECTION 1:

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To BIG Language Solutions, LLC:

Scope

We have examined the accompanying description of BIG Language Solutions, LLC's ("BIG Language Solutions") Translation Application Services system throughout the period March 1, 2024 to February 28, 2025, based on the criteria for a description of a service organization's system in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)* (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 1, 2024 to February 28, 2025, to provide reasonable assurance that BIG Language Solutions' service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

BIG Language Solutions uses Amazon Web Services, Inc., Google LLC, Microsoft Corporation, MongoDB, Inc., and SendGrid, Inc., sub-service organizations, for cloud storage services, cloud hosting and managed services, virtual desktop infrastructure services, database hosting services, and transactional email services, respectively. The description indicates that complementary sub-service organization controls that are suitably designed and operating effectively are necessary, along with controls at BIG Language Solutions, to achieve BIG Language Solutions' service commitments and system requirements based on the applicable trust services criteria. The description presents BIG Language Solutions' controls, the applicable trust services criteria, and the types of complementary sub-service organization controls assumed in the design of BIG Language Solutions' controls. The description does not disclose the actual controls at the sub-service organizations. Our examination did not include the services provided by the sub-service organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary sub-service organization controls.

The information included in Section 5, *Information provided by the Service Organization Not Covered by the Service Auditor's Report*, is presented by management of BIG Language Solutions to provide additional information and is not a part of the description. Management's responses to the testing exceptions included in Section 5 have not been subjected to the procedures applied in the examination of the description, and of the suitability of the design and operating effectiveness of controls to achieve BIG Language Solutions' service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

Service Organization's Responsibilities

BIG Language Solutions' management 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 BIG Language Solutions' service commitments and system requirements were achieved. BIG Language Solutions' management has provided the accompanying assertion titled "Management of BIG Language Solutions, LLC's Assertion" included in Section 2 of this report about the description and the suitability of design and operating effectiveness of controls stated therein. Management 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 Auditor's 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 American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated 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 a description of a service organization's system and the suitability of the design and operating effectiveness of the controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- 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
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- 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
- 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
- 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 users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusion about the suitability of the design or operating effectiveness of controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4 of this report.

Basis for a Qualified Opinion

The description of the Translation Application Services system describes the user termination processes in place to revoke system access upon termination of employment. However, as noted in the testing results of the control (CTL-050) within Section 4, *Categories, Criteria, Control Descriptions, Related Controls and Tests of Operating Effectiveness*, exceptions were noted. As a result, the control was not operating effectively to meet the following criteria:

- 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.
- 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 description of the system describes the infrastructure change management process in place to test, document, and approve changes prior to implementation. However, as noted in the testing results of the control (CTL-081) within Section 4, *Categories, Criteria, Control Descriptions, Related Controls and Tests of Operating Effectiveness*, a complete and accurate population of infrastructure changes was unable to be obtained. As a result, the control was not operating effectively to meet the following criterion:

- 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.

Opinion

In our opinion, except for the possible effects of the matters described in the preceding paragraphs, in all material respects:

- a. the description presents BIG Language Solutions' Translation Application Services system that was designed and implemented throughout the period March 1, 2024 to February 28, 2025, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period March 1, 2024 to February 28, 2025, to provide reasonable assurance that BIG Language Solutions' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the sub-service organizations applied the complementary controls assumed in the design of BIG Language Solutions' controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period March 1, 2024 to February 28, 2025, to provide reasonable assurance that BIG Language Solutions' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary sub-service organization controls assumed in the design of BIG Language Solutions' controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of BIG Language Solutions, user entities of BIG Language Solutions' Translation Application Services system during some or all of the period March 1, 2024 to February 28, 2025, business partners of BIG Language Solutions subject to risks arising from interactions with the Translation Application Services 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:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, sub-service organizations, and other parties
- Internal control and its limitations
- Complementary sub-service 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
- The applicable trust services criteria
- 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.



June 3, 2025
St. Petersburg, Florida

SECTION 2:

MANAGEMENT'S ASSERTION

MANAGEMENT OF BIG LANGUAGE SOLUTIONS, LLC'S ASSERTION

June 3, 2025

We have prepared the accompanying description of BIG Language Solutions, LLC's ("BIG Language Solutions") Translation Application Services system throughout the period March 1, 2024 to February 28, 2025, based on the criteria for a description of a service organization's system in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about the Translation Application Services system that may be useful when assessing the risks arising from interactions with BIG Language Solutions' system, particularly information about system controls that BIG Language Solutions has designed, implemented, and operated to provide reasonable assurance that our service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

BIG Language Solutions uses Amazon Web Services, Inc., Google LLC, Microsoft Corporation, MongoDB, Inc., and SendGrid, Inc., sub-service organizations, for virtual desktop infrastructure services, cloud hosting and managed services, database hosting services, and transactional email services, respectively. The description indicates that complementary sub-service organization controls that are suitably designed and operating effectively are necessary, along with controls at BIG Language Solutions, to achieve BIG Language Solutions' service commitments and system requirements based on the applicable trust services criteria. The description presents BIG Language Solutions' controls, the applicable trust services criteria, and the types of complementary sub-service organization controls assumed in the design of BIG Language Solutions' controls. The description does not disclose the actual controls at the sub-service organizations.

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

- a. the description presents BIG Language Solutions' Translation Application Services system that was designed and implemented throughout the period March 1, 2024 to February 28, 2025, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period March 1, 2024 to February 28, 2025, to provide reasonable assurance that BIG Language Solutions' service commitments and system requirements would be achieved based on the applicable trust services criteria, if our controls operated effectively throughout the period, and if the sub-service organizations applied the complementary controls assumed in the design of BIG Language Solutions' controls throughout that period.
- c. except for the matters described in paragraphs d. and e. below, the controls stated in the description operated effectively throughout the period March 1, 2024 to February 28, 2025, to provide reasonable assurance that BIG Language Solutions' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary sub-service organization controls assumed in the design of BIG Language Solutions' controls operated effectively throughout that period.
- d. our description of the Translation Application Services system describes the user termination process in place to revoke system access upon termination of employment. However, as noted in the testing results of the control (CTL-050) within Section 4, exceptions were noted. As a result, the control was not operating effectively to meet the following criteria:
 - 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.

- 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.
- e. our description of the system describes the infrastructure change management process in place to test, document, and approve changes prior to implementation. However, as noted in the testing results of the control (CTL-081) within Section 4, *Categories, Criteria, Control Descriptions, Related Controls and Tests of Operating Effectiveness*, a complete and accurate population of infrastructure changes was unable to be obtained.

/s/ BIG Language Solutions, LLC

Dave Perlman – Chief Executive Officer

Dan Nelson – Chief Technology Officer

SECTION 3:

DESCRIPTION OF THE SYSTEM

SCOPE OF REPORT AND DISCLOSURES

Overview

This description of the system of controls provided by BIG Language Solutions, LLC's ("BIG Language Solutions") management, as related to Statement on Standards for Attestation Engagements No. 21 '*Direct Examination Engagements*', specifically AT-C Section 105, '*Concepts Common to All Attestation Engagements*' and AT-C Section 205, '*Assertion – Based Examination Engagements*,' considers the direct and indirect impact of risks and controls that BIG Language Solutions management has determined are likely to be relevant to its user entities' internal controls intended to mitigate risks related to security, availability, processing integrity, confidentiality, or privacy.

Trust Services Categories and Related Criteria

The five attributes of a system are known as *categories*, and they are defined as follows:

- **Security:** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

Security refers to the protection of

- i. information during its collection or creation, use, processing, transmission, and storage and
- ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

- **Availability:** Information and systems are available for operation and use to meet the entity's objectives.

Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

- **Processing Integrity:** System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether the system achieves the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation. Because of the number of systems used by an entity, processing integrity is usually only addressed at the system or functional level of an entity.

- **Confidentiality:** Information designated as confidential is protected to meet the entity's objectives.

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

- **Privacy:** Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

Although the confidentiality criteria apply to various types of sensitive information, privacy applies only to personal information.

The privacy criteria are organized into eight categories:

- a. *Notice and communication of objectives.* The entity provides notice to data subjects about its objectives related to privacy.
- b. *Choice and consent.* The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.
- c. *Collection.* The entity collects personal information to meet its objectives related to privacy.
- d. *Use, retention, and disposal.* The entity limits use, retention, and disposal of personal information to meet its objectives related to privacy.
- e. *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.
- f. *Disclosure and notifications.* The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.
- g. *Quality.* The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy.
- h. *Monitoring and enforcement.* The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

The trust services criteria may be used when evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the entity. As such, they may be used when evaluating whether the entity's controls were effective to meet the criteria relevant to any of those categories, either individually or in combination with controls in other categories.

Scope

The scope that management has determined appropriate for the Translation Application Services system includes the controls to meet the applicable trust services criteria. Management is responsible for the identification of risks associated with the system of controls, and for the design and operation of controls intended to provide reasonable assurance that the applicable trust services criteria would be met.

As part of its overall SOC 2® program, BIG Language Solutions' management sets and determines the scope and timing of each report. This description of the system has been prepared by BIG Language Solutions' management, headquartered in Atlanta, Georgia, to provide information on controls applicable to meet the trust services criteria for Security.

Sub-Service Organizations

BIG Language Solutions uses Amazon Web Services, Inc. ("AWS"), Google LLC ("GCP"), Microsoft Corporation ("Azure"), MongoDB, Inc. ("MongoDB"), and SendGrid, Inc. ("SendGrid"), sub-service organizations, for cloud storage services, cloud hosting and managed services, virtual desktop infrastructure services, database hosting services, and transactional email services, respectively.

The description indicates that complementary sub-service organization controls that are suitably designed and operating effectively are necessary, along with controls at BIG Language Solutions, to achieve BIG Language Solutions' service commitments and system requirements based on the applicable trust services criteria. The description presents BIG Language Solutions' controls, the applicable trust services criteria, and the types of complementary sub-service organization controls assumed in the design of BIG Language Solutions' controls. The description does not disclose the actual controls at the sub-service organizations. This examination did not include the services provided by the sub-service organizations and did not include an evaluation of the suitability of the design or operating effectiveness of such complementary sub-service organization controls.

Significant Changes during the Examination Period

Management is not aware of any significant changes that occurred during the examination period.

Subsequent Events

Management is not aware of any relevant events that occurred subsequent to the period covered by management's description included in Section 3 of this report through the date of the service auditor's report that would have a significant effect on management's assertion.

System Incidents

Management is not aware of any system incidents that (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more service commitments and system requirements during the period covered by management's description included in Section 3 of this report.

Using the Work of the Internal Audit Function

The service auditor did not utilize any work of an Internal Audit function in preparing this report.

OVERVIEW OF OPERATIONS AND THE SYSTEM

Company Overview and Background

BIG Language Solutions was founded in partnership with MSouth Equity Partners, a private equity firm, with the underlying strategy of gaining a foothold within the global language industry. BIG Language Solutions provides professional translation services to its customers in over 200 languages and dialects. Their in-house linguists work with a worldwide alliance of translators, proofreaders, interpreters, localization specialists, and editors to deliver professional translation services across any media. BIG Language Solutions works with customers in a variety of industries such as Insurance, Healthcare, Legal, Entertainment, Consumer Products and Retail, and Manufacturing.

Overview of the Translation Application Services System

BIG Language Solutions' web portal is a translation management system (known as LanguageVault®) that allows customer contacts, contractors, and staff to work collaboratively to deliver secure translations. Customers log in to the LanguageVault® web portal to submit their translation requests. BIG Language Solutions employees and contractor users access the web portal to work on translation projects. The application solution was architected with data confidentiality and security as core components of development. When customers send confidential information, Internet Protocol (IP) whitelisting is utilized so project files can be uploaded into the web portal from known sources. Once uploaded, BIG Language Solutions staff and contractors remote into an IP whitelisted, secure virtual desktop managed via Microsoft's Azure Virtual Desktops (AVD) solution where project files are able to be downloaded and worked on.

Principal Service Commitments and System Requirements

BIG Language Solutions' security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided on BIG Language Solutions' website. Security commitments are standardized and include, but are not limited to, the following:

Trust Services Category	Service Commitments	System Requirements
Security	➤ System access is granted to authorized personnel only ➤ Identification and remediation of security incidents / events ➤ Protection of online and offline offerings that may contain customers' personal data ➤ Secure application development ➤ Secure customer personal information from accidental loss and unauthorized access, use, alteration, and disclosure	➤ Logical access standards ➤ Encryption standards ➤ Ongoing monitoring of security infrastructure and incident response process ➤ Data access based on principles of least privilege ➤ Secure web portal to maintain data ➤ Application and network vulnerability standards

BIG Language Solutions regularly reviews product security and performance metrics to ensure these commitments are met. In the event that material changes decreasing the level of security are made to the agreement, BIG Language Solutions will notify the customer through email or other means.

BIG Language Solutions establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated within their system policies and procedures and public-facing website. Information security policies define an organization-wide approach to how systems and data are protected. These include policies on how the platform is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the BIG Language Solutions web portal. Infrastructure systems are designed to eliminate single points of failure with dual circuits, switches, networks, and other necessary components to provide redundancy.

In accordance with Big Language Solutions' assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to system users, in each individual case.

OVERVIEW OF RELEVANT INFRASTRUCTURE

The Translation Application Services system is comprised of the following components:

- Infrastructure – the physical structures, information technology (IT), and other hardware
- Software – the application programs and IT system software that supports application programs
- People – the personnel involved in the governance, operation, and use of a system
- Procedures – the automated and manual procedures
- Data – transaction streams, files, databases, tables, and output used or processed by the system

Infrastructure

BIG Language Solutions' LanguageVault® solution is hosted within GCP utilizing Google Kubernetes Engine (GKE) and consists of a multi-tier virtualized architecture comprised of web and database servers, storage and content delivery systems, network and application monitoring, and logging tools. BIG Language Solutions utilizes AVD for their virtual desktop infrastructure. AWS' Simple Storage Service (S3) is also utilized for data archival. BIG Language Solutions does not own or maintain the hardware located in the Azure, GCP, and AWS data centers, and operates under a shared security responsibility model, where Azure, GCP, and AWS are responsible for the security of the underlying cloud infrastructure (physical infrastructure, geographical regions, availability zones, edge locations) and BIG Language Solutions is responsible for securing the platform deployed in Azure, GCP, and AWS (customer data, applications, identity access management, operating system, network security group configuration, network traffic, server-side encryption).

The AVD relies on Microsoft Entra to provide multifactor authentication (MFA) support. MongoDB Atlas is used to host the databases, and SendGrid is utilized for transactional emails. Data uploaded to LanguageVault® is encrypted using Google Cloud Storage (GCS) when being stored.

The following describes the in-scope components supporting the Translation Application Services system:

System / Application	Description	Infrastructure
Virtual Desktops	The virtual desktops are a Platform as a Service (PaaS) provided via AVD.	Cloud Hosted Using Windows Operating Systems
AWS S3	Used for archiving data.	Cloud Hosted
GKE	Provides a managed environment for deploying, managing, and scaling applications using Google infrastructure within GCP.	GCP
GCS	Files are stored and retrieved from GCS buckets. Google supports only encrypted storage.	GCP
MongoDB Atlas	Hosts the LanguageVault® database within GCP.	Cloud Hosted
SendGrid	Cloud-based email delivery service. Transactional emails are sent using TLS which provides end-to-end communications security over communication networks.	Cloud Hosted

Software

BIG Language Solutions' system refers to the guidelines and activities for providing transaction processing and other services to user entities and includes the infrastructure and software that support BIG Language Solutions' Translation Application Services system. The following software is used to support the Translation Application Services system:

- Microsoft Entra – Used to authenticate users and enforce MFA on virtual desktops or when accessing corporate resources, such as email or OneDrive.
- Jira – Ticketing system for tracking changes to the application and infrastructure.
- BitBucket – LanguageVault® source code repository and versioning system.
- Google Authenticator – Used to authenticate users to the GCP cloud environment accounts.
- Google Cloud Monitoring – Observability tooling for metrics, logging, and alerting.
- Microsoft Defender – Used to scan endpoint devices for malware.
- Google Cloud Security – Protects data using layered encryption, strong access controls, and continuous threat detection.

People

The overall organization supports the framework for an effective control environment. The roles and responsibilities of key functions include the following:

- Executive Management – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
- Human resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development) and for maintaining compliance with applicable employment regulations.
- Compliance – responsible for risk management and in conjunction with the security team; identification, monitoring, and compliance of security issues and incidents throughout the service delivery infrastructure.
- Information Technology (IT) Security and Operations – responsible for the development of new features and functions of the service and maintaining the technology supporting the platform.

Procedures

BIG Language Solutions' management is responsible for maintaining and implementing information technology general computer controls related to computer processing supporting the Translation Application Services system. These controls provide the basis for reliance on information / data from the systems used by user entities.

BIG Language Solutions maintains a set of policies, processes, and procedures that establish the rules of conduct within the organization and outline the responsibilities of employees, contractors, and employers as well as prevent, detect, and treat violations and risks. These policies and procedures are updated annually, communicated company wide, and are acknowledged by BIG Language Solutions employees to ensure awareness of their responsibilities. The following policies contain relevant controls:

- | | |
|--|------------------------------|
| ➤ Information Security Policy | ➤ Data Classification Policy |
| ➤ Business Continuity Plan | ➤ Incident Response Policy |
| ➤ Change Management Policy | ➤ Risk Management Policy |
| ➤ Disaster Recovery Plan | ➤ Vendor Management Policy |
| ➤ Data Protection and Destruction Policy | ➤ Asset Management Policy |
| ➤ Encryption Policy | ➤ Code of Conduct |

Information Security

Information security policies have been established to set the overall framework for managing security of the IT infrastructure and applications supporting BIG Language Solutions' services. These policies are approved at the executive management level and establish standards for information security throughout the organization. User administration processes for IT systems and applications are tied to the new hire and termination processes established by BIG Language Solutions. Access is assigned based on personnel job responsibilities. To reinforce awareness and compliance, employees and contractors are required to acknowledge their review of the Information Security Policy on an annual basis. This annual review ensures personnel remain informed of the company's expectations and any updates to the policy.

Access Authentication and Authorization

Prior to accessing system information, including confidential information, users first have to connect to the AVD. The AVD is protected by authentication and authorization mechanisms via Microsoft Entra. The operations and security teams are responsible for assigning and maintaining access rights to the production environment. In order to gain access to the production environment a user is required to authenticate first to the virtual desktops, then via MFA in order to enforce public-private key authentication. To access the production databases, users are required to authenticate with a username and password. In addition, administrative access privileges within the production environment are restricted to personnel commensurate with their job responsibilities. Production resources are protected by network security group rulesets designed to filter unauthorized Internet traffic and to deny any activity not previously defined.

Access Requests and Access Revocation

Management has established controls to ensure that access to confidential data is restricted to those who require access. A formal process has been established for managing user accounts and controlling access to BIG Language Solutions resources within the production environment. New employees are granted a standard level of access based on their job role. Prior to granting individual access above the standard level of access provided upon employment, the access request is then to be reviewed and approved by the employee's manager. Upon notification of an employee termination, HR personnel create a termination checklist which is shared with the IT department to ensure that employees do not retain system access subsequent to their termination date. Management requires access requests and access revocations to be formally documented to ensure activities are completed for the addition, modification, and revocation of system and software access privileges. On a monthly basis, BIG Language Solutions security and IT teams perform a user access review to verify users with access to the productions systems are authorized.

Change Management

BIG Language Solutions has documented application change management and infrastructure maintenance policies and procedures to communicate management's expectations regarding the change control process to personnel to help ensure unauthorized changes are not made to production systems. These policies and procedures apply to changes including, but not limited to, application changes, emergency changes, and infrastructure changes. These policies convey the change control process including, as necessary, maintenance procedures, rollback procedures, assessing the impact of changes, test plans, and approvals.

Production changes are documented and tracked within a ticketing system. Separate development, test, and production environments are maintained. By policy, changes are tested in a logically separated test environment prior to implementation to the production environment. The production change request process enforces and records request authorization, code review and testing (where applicable), migration approval, and implementation. Approval for releases is obtained prior to moving the changes to production. Approved changes are performed or managed directly by authorized IT personnel. In some instances, there are changes that cannot be tested prior to implementation. In those instances, validation is performed once the change is completed, and documentation is retained within the ticketing system.

In the event that implementation of an emergency change is necessary, the change is required to follow the established change control process. A third-party version control software is utilized to control access to source code and provide version control for application changes. Administrative access privileges and the ability to modify the source code library within the version control software are restricted to authorized IT personnel.

In addition, change management personnel involved in the change management process maintain a continuous discussion channel to discuss upcoming changes, change prioritization, and to approve application change requests. Application changes that may have an impact on the customer will be communicated internally to management and to customers prior to deployment.

Data Backup and Disaster Recovery

Documented backup procedures are in place to guide personnel in data backup and retention activities. IT personnel utilize automated backup systems to perform backups of the production data and servers on predefined schedules. Restorations from backup media are performed as a component of normal business operations to verify that certain system components can be recovered from backup media. Additionally, the RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are both 24 hours. A disaster recovery test exercise is conducted on an annual basis to ensure the disaster recovery procedures are capable of meeting the defined RTOs and RPOs.

Incident Response

Incident response and escalation policies and procedures are in place to manage unexpected incidents impacting the business. The incident response process defines activities for identifying and mitigating security breaches. Management utilizes a ticketing system to manage, track, and respond to incidents until resolution. When an issue is detected, the IT team will examine and attempt to troubleshoot the issue. If the IT employee cannot resolve the issue, the ticket is escalated and assigned to the appropriate group. Management utilizes a customer service system and email for communicating and collaborating to resolve identified incidents with customers. The IT team is responsible for the identification, resolution, and communication of security related incidents to impacted parties; and customers are responsible for reporting issues based on the terms of the service agreements. Additionally, an internal collaboration tool is accessible by internal users to report incidents, concerns, and complaints.

System Monitoring

BIG Language Solutions has implemented data communications policies and procedures to guide personnel in managing security infrastructure and maintaining data integrity and security during transmission. These policies address topics that include, but are not limited to, the following:

- Firewall systems
- Intrusion detection systems (IDS)
- Remote access
- Encryption

The IT team is responsible for assembling, operating, securing, and monitoring the performance of infrastructure resources, including the hardware, dependent services, and logical configurations of the production environment. A performance monitoring tool is utilized to monitor the system uptime and performance, where administrators can review throughput, aggregate database query performance, and other related activities to support the operations team in making decisions to determine whether to add additional computing resources to improve performance. The standard uptime for the application is 24 x 7 x 365.

Vulnerability Management

BIG Language Solutions has established a vulnerability management program that details the procedures for identifying and addressing security vulnerabilities. This includes management reviews of specific applications and dashboards that monitor for and track the remediation of suspicious activities and anomalies. The review process incorporates findings from static and dynamic application security testing (SAST and DAST), container image scans, findings from penetration tests and network vulnerability scans, and analyses of significant incidents reported by the security event and log management system to ensure vigilant monitoring of critical security threats. Additionally, the firewall ruleset is reviewed by the security team on a weekly basis to ensure that allowed routes have an active business justification.

Endpoint Protections

The organization has an Acceptable Use Policy in place that defines what the employees' responsibilities and boundaries are when it comes to the use of technology and information systems within the environment of the organization. The antivirus solution provides real-time monitoring and protection from malicious code and viruses. Virus signatures and definition files are automatically updated on registered clients on a daily basis. Sensitive data on virtual workstations is automatically hidden after fifteen minutes of inactivity and requires the user to re-authenticate thereafter. In the event of loss, theft, or other physical compromise of employee laptops, full disk encryption software is in place to protect data from unauthorized access.

Data

Communications between the end user and the LanguageVault® application are encrypted using Hypertext Transfer Protocol Secure (HTTPS) over TLS 1.2 and TLS 1.3 encryption protocols and a network diagram is used to illustrate the segmentation boundaries and communication paths between system resources. Amazon Workspaces is implemented to create a secure data environment that prevents data being transferred outside of the environment.

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

Classification	Data Description	Data Reporting
Restricted	Highly sensitive data that should not leave BIG Language Solutions' managed systems.	Customer output / data is available only from restricted workspaces managed by BIG Language Solutions and machines managed by the customer.
Confidential	Sensitive data that could leave BIG Language Solutions' managed systems only over secure communications channels.	Customer output / data might be available from selected machines not necessarily managed by BIG Language Solutions or managed by the customer.
Public	Non-sensitive data that may be publicly published and available.	Customer output / data is publicly available.

RELEVANT ASPECTS OF CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATIONS SYSTEMS, AND MONITORING

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal controls, providing discipline and structure. Aspects of BIG Language Solutions' control environment that affect the services provided and / or the system of controls are identified in this section.

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 BIG Language Solutions' control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of BIG Language Solutions' ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. 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. Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures, including an employee disciplinary policy that communicates repercussions for noncompliance. Employees and contractors are required to review and acknowledge the code of conduct, which describes possible sanctions for violations of, as a component of the onboarding process and annually thereafter.

Upon hire, BIG Language Solutions personnel receive an employee handbook that includes information about the company's vision, mission, core values, and culture. Attention is also devoted to reviewing the code of business conduct. BIG Language Solutions has established and maintains a formal Code of Conduct that outlines expectations for professional behavior and ethical standards within the workplace. This document governs employee and contractor conduct and is intended to foster an environment of integrity, respect, and accountability.

Board of Directors / Executive Management

BIG Language Solutions' control consciousness is influenced significantly by the participation of its executive management and Board of Directors (BoD). The BoD follows a formal charter and an established set of bylaws when fulfilling their responsibilities and oversight of management's system of internal control. The BoD maintains sufficient independence from operations management to remain objective in evaluations and decision making. Attributes include the experience and stature of its members, the extent of its involvement and scrutiny of activities and the suitability of its actions. The executive management team comprised of security personnel and executive staff meets and interacts with team members as a component of day-to-day operations to discuss business objectives and operational issues. The BoD meets on a quarterly basis to discuss business objectives and strategic direction of the company, and the executive management team will present internal control performance metrics to the BoD once per year. The audit committee, along with executive management, provides oversight of the audit process, the company's system of internal controls, and compliance with laws and regulations.

Commitment to Competence

BIG Language Solutions' management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. BIG Language Solutions' commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Management has considered the competence levels for jobs and translated required skills and knowledge levels into written position requirements. BIG Language Solutions also offers training courses to employees to maintain and advance the skill level of personnel. To facilitate the hiring of appropriately skilled and qualified employees, Human Resources has implemented formal hiring procedures to guide the hiring process. Background screenings are performed for employees and contractors as a component of the onboarding process to validate their qualifications.

and mitigate hiring risks. In addition, employees are required to complete security awareness training upon hire and again on an annual basis to understand their obligations and responsibility to comply with security policies.

Management's Philosophy and Operating Style

BIG Language Solutions' management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward information processing, accounting functions, and personnel. A specific control activity that BIG Language Solutions has implemented in this area is that management provides internal control performance results to the BoD on an annual basis for review. A disciplinary policy is in place that includes disciplinary action up to, and including, termination for violation of company policies or procedures. Additionally, each year employees receive a performance review by their managers to assess their performance against a set of standards for the company.

Organizational Structure

BIG Language Solutions' organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. BIG Language Solutions' management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and applicable lines of reporting. BIG Language Solutions has developed an organizational structure suited to its needs. This organizational structure is based in part on its size and the nature of its activities. Organizational charts are in place to communicate key areas of authority, responsibility, and applicable lines of reporting to personnel. These charts are communicated to employees via SharePoint and updated on an as needed basis. Supporting these organizational charts are the job descriptions in place that define the specific skills, responsibilities and knowledge levels required for certain positions.

Human Resource Policies and Practices

BIG Language Solutions' HR policies and practices are clearly written and communicated where appropriate. Policies and procedures that are listed in the employee handbook include hiring, training, disciplinary actions, and termination procedures. Prior to accessing the system, employees and contractors have to sign a confidentiality agreement during the onboarding process. This agreement affirms their responsibility to protect proprietary and sensitive information from unauthorized access or disclosure.

Risk Assessment

BIG Language Solutions has placed a risk assessment process in operation to identify and manage risks that could affect the organization's ability to provide reliable services for its user entities. This process requires management to identify significant risks in their areas of responsibility and to implement measures to address those risks. Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security category.

Objective Setting

BIG Language Solutions' service commitments and related requirements are documented and reviewed by management during the risk assessment process to ensure these commitments are met in the design and operation of internal controls. On an annual basis, management evaluates and presents the results of controls and compliance assessments and recommended initiatives to executive management to ensure the operations, reporting, and compliance objectives are aligned with the company's mission and are being met. Management also reviews vendor audit reports on an annual basis to ensure that third-party providers are in compliance with the organization's requirements.

Risk Identification and Analysis

BIG Language Solutions has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its customers. Key members of the audit committee, executive management, and operational teams meet on an annual basis to identify and review risks to the system and opportunities for BIG Language Solutions. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring, and identification of the control activities necessary to mitigate the risk. These discussions culminate in the creation of a risk and opportunities assessment framework. Other inputs into these risk discussions are the potential impacts of developing technologies, the constant changing landscape of regulatory and legislative requirements, and the monthly reviews of the operating effectiveness of key controls.

Risk Factors

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

External Factors

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

Internal Factors

- Significant changes in policies, processes, or personnel
- A disruption in information systems processing
- The quality of personnel hired and methods of training utilized
- Changes in management responsibilities
- Types of fraud: (1) Fraud incentives and pressures for employees; (2) Fraud opportunities; (3) Employee attitudes and rationalizations for fraud.

Potential for Fraud

Management considers the potential for fraud when assessing the risks to the company's objectives. Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. Additionally, the risk assessment that considers the potential for fraud is performed on an annual basis.

Risk Mitigation

As a result of the annual risk assessment process, management formulates a risk treatment plan that documents risk treatment decisions including designed control activities to mitigate risks to defined risk tolerance levels. Management also documents mitigation plans to guide personnel in procedures to protect against disruptions caused by an unexpected event. Vendor evaluations are conducted as part of the vendor selection process, and management also reviews audit reports from current vendors to help ensure they maintain compliance with security commitments.

Information and Communication Systems

Information System

BIG Language Solutions utilizes various tools for the monitoring of production systems that allow information to be identified and communicated in sufficient detail and in a timeframe that allows employees to carry out their responsibilities. BIG Language Solutions' information systems provide information to help identify risks and opportunities, and high-quality information to manage and control activities. Information systems are relied upon for the achievement of company-level and process / application-level objectives.

Communication System

Internal Communications

BIG Language Solutions has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include:

- Ensuring documented policies and procedures are in place to guide personnel in the entity's security commitments and that they are communicated to internal personnel.
- Requiring security awareness training to be completed upon hire and on an annual basis.
- Maintaining documented job descriptions to establish and define the structure, reporting lines, and authorities and responsibilities for employment positions.
- Having an implemented internal collaboration tool that is accessible by internal users to report incidents, concerns, and complaints.

External Communications

BIG Language Solutions has also implemented various methods of communications to help ensure that customers understand the role and responsibilities of BIG Language Solutions and to help ensure that significant events are communicated to customers in a timely manner. A support site is available to customers that contains general information such as production documentation, administrations, and how-to guides. BIG Language Solutions utilizes the public facing website to communicate relevant information regarding the design and operation of the system and BIG Language Solutions' commitments to external customers. Customers are encouraged to communicate questions and problems (including incidents) through the BIG Language Solutions web portal site, and such matters are logged and tracked until resolved, with the resolution also reported to the customer.

Monitoring

BIG Language Solutions' management performs monitoring activities in order to continuously assess the quality of internal controls over time. Monitoring activities are used to initiate corrective action through department meetings, customer conference calls, and informal notifications. Management performs monitoring activities on a continuous basis and necessary corrective actions are taken as required to correct deviations from company policy and procedures. Management is responsible for directing and controlling operations and for establishing, communicating, and monitoring control activities and procedures. BIG Language Solutions management places emphasis on maintaining sound internal controls, as well as ensuring integrity and ethical values to personnel.

On-Going Monitoring

BIG Language Solutions management performs monitoring activities to assess the quality of internal control over time and monitors activities throughout the year and takes corrective actions to address deviations from company policy and procedures. Management utilizes a risk-based approach to monitor business units and other auditable entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed in order of significance.

Support personnel monitor customer communications. This information is provided to management providing the ability to track, monitor and assist in understanding customer complaints, concerns, and to evaluate and resolve special requests in a timely fashion. Management's ability to actively monitor customer's communications is an integral role in controlling the quality of the services provided.

Management is proactive in responding to customer complaints and there is a high level of inter-departmental communication about these events. Customer complaints and other issues are handled via an internal ticketing system and by personal contact by management staff.

Vendor and Sub-Service Organization Monitoring

BIG Language Solutions management reviews documentation provided by third-party providers on an annual basis to help ensure that cloud hosting services are in compliance with security policies, including pre-defined performance metrics. If issues are detected during the course of the stated monitoring activities, BIG Language Solutions management follows up with the subservice organization until the issue is resolved.

Documentation that is reviewed by BIG Language Solutions management includes, but is not limited to, the following:

- Annual Service Auditor reports
- International Organization for Standardization (ISO) 27001 certifications
- Master Service Agreements (MSAs) and SLAs

Separate Evaluations

Management has implemented a self-assessment program to evaluate the performance of specific control activities and processes over time and confirm that the in-scope controls were consistently applied as designed, including whether manual controls were applied by individuals who have the competence and authority. As a result of management's risk analysis process, each control activity within scope has been assigned a risk level associated with the assessed level of risk it is intended to mitigate. Controls that serve to mitigate multiple risks are assigned the highest level of assessed risk among the pertinent risks.

Management has determined that each risk assignment or category will require structured inquiry, observation, inspection, or sample testing, or a combination of the aforementioned, based on the assigned risk level and the nature of the control, whether automated or manual, and the frequency of application (e.g., constant, daily, weekly, quarterly, etc.). For manual controls, the self-assessment is performed by a secondary individual different from the individual that primarily applies the control; additionally, subordinates do not evaluate the application of manual controls performed by their supervisors or managers. Additionally, an internal audit program with documented policies and procedures is in place to outline the required methods for monitoring, measurement, scope, and frequency for security reviews.

Evaluating and Communicating Deficiencies

Management has developed protocols to help ensure findings of internal control deficiencies should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables the individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Deficiencies found via the ongoing monitoring activities are further investigated by BIG Language Solutions' management and are tracked from identification to resolution.

CATEGORIES, CRITERIA, AND RELATED CONTROLS

The categories, criteria, and related controls are included in Section 4 of this report, “Categories, Criteria, Related Controls and Tests of Operating Effectiveness”, to eliminate the redundancy that would result from listing them in this section and repeating them in Section 4. Although the criteria and related controls are included in Section 4, they are, nevertheless, an integral part of the organization’s description of controls.

COMPLEMENTARY CONTROL CONSIDERATIONS

BIG Language Solutions' controls do not depend on the implementation of Complementary User Entity Controls (CUECs) at user entities to meet their service commitments and requirements; however, user entities are responsible for performing certain activities to benefit from BIG Language Solutions' Translation Application Services system.

BIG Language Solutions' control policies and procedures were designed with the assumption that certain controls would be in place and in operation at the sub-service organizations. Sub-service organization controls must be evaluated, taking into consideration BIG Language Solutions' controls and their own internal controls. BIG Language Solutions' management does not make any representations regarding responsibility related to or provide any assurance regarding any such internal control or regulatory requirements for which the customer must assess or comply.

This section describes some of the control considerations for the sub-service organizations or "complementary controls", which should be in operation at the sub-service organizations and to complement the controls at the service organization. User auditors / user entities should determine whether the sub-service organizations have established controls to ensure that the criteria within this report are met. The "complementary controls" presented below should not be regarded as a comprehensive list of all controls that should be employed by the sub-service organizations.

Control Considerations for Sub-Service Organizations

1. Sub-service organizations are responsible for implementing control activities to provide reasonable assurance that backups are encrypted and retained.
2. Sub-service organizations are responsible for implementing control activities to provide reasonable assurance that critical IT infrastructure is protected from certain physical and environmental threats.
3. Sub-service organizations are responsible for implementing control activities to provide reasonable assurance that IT infrastructure is recoverable in the event of a disaster.
4. Sub-service organizations are responsible for responsible for implementing control activities to provide reasonable assurance that personnel are properly screened prior to being granted access to user entity systems.

SECTION 4:

CATEGORIES, CRITERIA, CONTROL DESCRIPTIONS, RELATED CONTROLS AND TESTS OF OPERATING EFFECTIVENESS

INFORMATION PROVIDED BY THE SERVICE AUDITOR

Introduction

This report is intended to provide user entities, prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding with information about controls that may affect the Translation Application Services system provided by BIG Language Solutions and to provide information about the operating effectiveness of controls that were tested.

The scope of our testing of BIG Language Solutions' controls was limited to the categories, criteria, and the related controls specified by BIG Language Solutions' management and contained within Section 4 of this report, which management believes to be the relevant key controls for the categories and criteria included in the scope of this report. Our review was not extended to controls in place at any user entities, sub-service organizations, or any other third-party vendors.

The examination was performed in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 21 '*Direct Examination Engagements*', specifically AT-C Section 105, "*Concepts Common to All Attestation Engagements*" and AT-C Section 205, '*Assertion – Based Examination Engagements*.' It is each interested party's responsibility to evaluate this information in relation to controls in place at user entities and sub-service organizations to obtain an overall understanding of internal control and to assess control risk. Controls in place at user entities, sub-service organizations, and BIG Language Solutions must be evaluated together. A general, but not inclusive, listing of control considerations is provided in Section 3, "Complementary Control Considerations." If an effectively operating user entity or sub-service organization internal control is not in place, the controls at BIG Language Solutions may not sufficiently compensate for the deficiency.

Tests of Operating Effectiveness

Our tests of the operating effectiveness of the controls specified by BIG Language Solutions' management included such tests as we considered necessary in the circumstances to obtain reasonable, but not absolute, assurance that the controls operated in a manner that achieved the specified criteria during the period from March 1, 2024 to February 28, 2025. In selecting particular tests of the operating effectiveness of controls we considered 1) the nature of the controls being tested; 2) the types and completeness of available evidential matter; 3) the nature of the criteria to be achieved; 4) the assessed level of control risk; 5) the expected efficiency and effectiveness of the test; and 6) the testing of other controls relevant to the criteria.

Testing exceptions, if any, and information about specific tests of the operating effectiveness performed that may be relevant to the interpretation of testing results by user entities, prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding for the controls specified to achieve the criteria are presented in this section under the column heading "Results of Testing." The concept of materiality is not applied when reporting the results of the tests of controls for which exceptions have been identified because the independent service auditor does not have the ability to determine whether an exception will be relevant to a particular user entity. Consequently, 360 Advanced, Inc. reports all exceptions. Exceptions identified herein are not necessarily considered significant deficiencies or material weaknesses in the total system of internal controls of BIG Language Solutions, as this determination can only be made after consideration of controls in place at user entities. Control considerations that should be exercised by BIG Language Solutions' clients to complement the controls of BIG Language Solutions to attain the criteria are presented in relation to the nature of services being audited and the controls specified by BIG Language Solutions management.

Types of Tests 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 appropriate personnel seeking relevant information or representation to obtain the following information about the control: ➤ Knowledge and additional information regarding the policy or procedure; and ➤ Corroborating evidence of the policy or procedure.
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
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed

Procedures for Assessing Completeness and Accuracy of IPE

For tests of controls requiring the use of Information Provided by the Entity (“IPE”) (e.g., controls requiring system generated populations for sample-based testing), 360 Advanced, Inc. performed a combination of the following procedures, where possible, based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspected the source of the IPE, (2) inspected the query, script, or parameters used to generate the IPE, (3) tied data between the IPE and the source, and / or (4) inspected the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintained its integrity. In addition to the above procedures, for tests of controls requiring management’s use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), the independent service auditor inspected management’s procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Sampling Methodology

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.

CATEGORIES, CRITERIA, AND RELATED CONTROLS

Security (Common Criteria to All Categories)

Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
Control Environment			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CTL-001	A code of conduct is in place to govern workplace behavior standards.	Inquired of the Director of Information Security & Compliance to verify that a code of conduct was in place to govern workplace behavior standards.	No exceptions noted.
		Inspected the code of conduct to verify that a code of conduct was in place to govern workplace behavior standards.	No exceptions noted.
CTL-003	Employees and contractors are required to review and acknowledge the code of conduct as a component of the onboarding process.	Inquired of the Director of Information Security & Compliance to verify that employees and contractors were required to review and acknowledge the code of conduct as a component of the onboarding process.	No exceptions noted.
		Inspected the acknowledged code of conduct within the employee handbook for a sample of employees and contractors onboarded within the examination period to verify that employees and contractors were required to review and acknowledge the code of conduct as a component of the onboarding process.	No exceptions noted.
CTL-004	Background screenings are performed for employees and contractors as a component of the onboarding process.	Inquired of the Director of Information Security & Compliance to verify that background screenings were performed for employees and contractors as a component of the onboarding process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the completed background screenings for a sample of employees and contractors onboarded within the examination period to verify that background screenings were performed for employees and contractors as a component of the onboarding process.	No exceptions noted.
CTL-005	Employees and contractors are required to sign and acknowledge a confidentiality statement agreeing not to disclose confidential information to unauthorized parties.	Inquired of the Director of Information Security & Compliance to verify that employees and contractors were required to sign and acknowledge a confidentiality statement agreeing not to disclose confidential information to unauthorized parties.	No exceptions noted.
		Inspected the acknowledged confidentiality agreements for a sample of employees and contractors onboarded within the examination period to verify that employees and contractors were required to sign and acknowledge a confidentiality statement agreeing not to disclose confidential information to unauthorized parties.	No exceptions noted.
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CTL-006	A Board of Directors is in place to exercise oversight of the development and performance of internal control.	Inquired of the Director of Information Security & Compliance to verify that a Board of Directors was in place to exercise oversight of the development and performance of internal control.	No exceptions noted.
		Inspected the charter to verify that a board of directors was in place to exercise oversight of the development and performance of internal control.	No exceptions noted.
CTL-007	The Board of Directors includes members who are independent from management, in accordance with the Board of Directors' bylaws, and are objective in evaluations and decision making.	Inquired of the Director of Information Security & Compliance to verify that the Board of Directors included members who were independent from management, in accordance with the Board of Directors' bylaws, and were objective in evaluations and decision making.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the listing of members and Board of Director bylaws to verify that the board of directors included members who were independent from management, in accordance with the Board of Directors' bylaws, and were objective in evaluations and decision making.	No exceptions noted.
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CTL-008	Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel and are communicated to employees.	Inquired of the Director of Information Security & Compliance to verify that organizational charts were in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel and were communicated to employees.	No exceptions noted.
		Inspected the organizational chart to verify that organizational charts were in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel and were communicated to employees.	No exceptions noted.
CTL-009	Documented job descriptions are in place to establish and define the structure, reporting lines, and authorities and responsibilities, for employment positions.	Inquired of the Director of Information Security & Compliance to verify that documented job descriptions were in place to establish and define the structure, reporting lines, and authorities and responsibilities, for employment positions.	No exceptions noted.
		Inspected the Information Security Officer job description to verify that documented job descriptions were in place to establish and define the structure, reporting lines, and authorities and responsibilities, for employment positions.	No exceptions noted.
CTL-010	An executive management team that is comprised of security personnel and executive staff has been established to guide the company in managing security risks.	Inquired of the Director of Information Security & Compliance to verify that an executive management team that was comprised of security personnel and executive staff had been established to guide the company in managing security risks.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected an executive management listing and meeting to verify that an executive management team that was comprised of security personnel and executive staff had been established to guide the company in managing security risks.	No exceptions noted.
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CTL-011	Policies and procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	Inquired of the Director of Information Security & Compliance to verify that policies and procedures were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties as outlined in the job description.	No exceptions noted.
		Inspected the Job Requisition and Recruiting SOP to verify that policies and procedures were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties as outlined in the job description.	No exceptions noted.
CTL-012	Annually, employees and contractors are required to complete security awareness training to comply with security policies.	Inquired of the Director of Information Security & Compliance to verify that employees and contractors were required to complete security awareness training to comply with security policies on an annual basis.	No exceptions noted.
		Inspected the completed security awareness training for a sample of employees and contractors active within the examination period to verify that employees and contractors were required to complete security awareness training to comply with security policies within the past 12 months.	No exceptions noted.
CTL-013	Employees and contractors are required to complete security awareness training as a component of the onboarding process.	Inquired of the Director of Information Security & Compliance to verify that employees and contractors were required to complete security awareness training as a component of the onboarding process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the acknowledged security awareness trainings for a sample of employees and contractors onboarded within the examination period to verify that employees and contractors were required to complete security awareness training as a component of the onboarding process.	No exceptions noted.
CTL-014	Training courses are made available to new and existing employees to maintain and advance the skill level of personnel.	Inquired of the Director of Information Security & Compliance to verify that training courses were made available to new and existing employees to maintain and advance the skill level of personnel.	No exceptions noted.
		Inspected the dashboard of the online learning portal to verify that training courses were made available to new and existing employees to maintain and advance the skill level of personnel.	No exceptions noted.
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CTL-003	Employees and contractors are required to review and acknowledge the code of conduct as a component of the onboarding process.	Inquired of the Director of Information Security & Compliance to verify that employees and contractors were required to review and acknowledge the code of conduct as a component of the onboarding process.	No exceptions noted.
		Inspected the acknowledged code of conduct within the employee handbook for a sample of employees and contractors onboarded within the examination period to verify that employees and contractors were required to review and acknowledge the code of conduct as a component of the onboarding process.	No exceptions noted.
CTL-015	Performance measures are in place that reflect required dimensions of performance and expected standards of conduct.	Inquired of the Director of Information Security & Compliance to verify that performance measures were in place that reflected required dimensions of performance and expected standards of conduct.	No exceptions noted.
		Inspected the employee handbook to verify that performance measures were in place that reflected required dimensions of performance and expected standards of conduct.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-016	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.	Inquired of the Director of Information Security & Compliance to verify that policies were documented and maintained that addressed remedial actions for lack of compliance with policies and procedures.	No exceptions noted.
		Inspected the Corrective Action Request Standard Operating Procedures and Code Of Conduct to verify that policies were documented and maintained that addressed remedial actions for lack of compliance with policies and procedures.	No exceptions noted.
Communication and Information			
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CTL-017	Information Security policies and procedures are in place to guide personnel.	Inquired of the Director of Information Security & Compliance to verify that information Security policies and procedures were in place to guide personnel.	No exceptions noted.
		Inspected the Information Security Policy to verify that information security policies and procedures were in place to guide personnel.	No exceptions noted.
CTL-018	Incident response and escalation policies are in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	Inquired of the Director of Information Security & Compliance to verify that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	No exceptions noted.
		Inspected the Incident Response SOP to verify that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	No exceptions noted.
CTL-027	The entity's information technology security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.	Inquired of the Director of Information Security & Compliance to verify that the entity's information technology security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Risk Assessment Tracker and a recent security alert to verify that the entity's information technology security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
CTL-062	Logging and monitoring applications are configured to collect data from system infrastructure components and used to monitor system performance, potential security threats and vulnerabilities, resource utilization and alert IT personnel upon detection of usual system activity or service requests.	Inquired of the Director of Information Security & Compliance to verify that logging and monitoring applications were configured to collect data from system infrastructure components and used to monitor system performance, potential security threats and vulnerabilities, resource utilization and alert IT personnel upon detection of usual system activity or service requests.	No exceptions noted.
		Inspected the logging and monitoring configurations to verify that logging and monitoring applications were configured to collect data from system infrastructure components and used to monitor system performance, potential security threats and vulnerabilities, resource utilization and alert IT personnel upon detection of usual system activity or service requests.	No exceptions noted.
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CTL-002	Annually, employees and contractors are required to acknowledge that the Information Security Policy was received and read.	Inquired of the Director of Information Security & Compliance to verify that employees and contractors were required to acknowledge that the Information Security Policy was received and read on an annual basis.	No exceptions noted.
		Inspected the Information Security Policy acknowledgements for a sample of employees and contractors active within the examination period to verify that employees and contractors were required to acknowledge that the Information Security Policy was received and read within the past 12 months.	Exceptions noted. 360 Advanced was unable to verify that the Information Security Policy was received and read for nine (9) out of the 29 employees and contractors selected.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-005	Employees and contractors are required to sign and acknowledge a confidentiality statement agreeing not to disclose confidential information to unauthorized parties.	Inquired of the Director of Information Security & Compliance to verify that employees and contractors were required to sign and acknowledge a confidentiality statement agreeing not to disclose confidential information to unauthorized parties.	No exceptions noted.
		Inspected the acknowledged confidentiality agreements for a sample of employees and contractors onboarded within the examination period to verify that employees and contractors were required to sign and acknowledge a confidentiality statement agreeing not to disclose confidential information to unauthorized parties.	No exceptions noted.
CTL-009	Documented job descriptions are in place to establish and define the structure, reporting lines, and authorities and responsibilities, for employment positions.	Inquired of the Director of Information Security & Compliance to verify that documented job descriptions were in place to establish and define the structure, reporting lines, and authorities and responsibilities, for employment positions.	No exceptions noted.
		Inspected the Information Security Officer job description to verify that documented job descriptions were in place to establish and define the structure, reporting lines, and authorities and responsibilities, for employment positions.	No exceptions noted.
CTL-012	Annually, employees and contractors are required to complete security awareness training to comply with security policies.	Inquired of the Director of Information Security & Compliance to verify that employees and contractors were required to complete security awareness training to comply with security policies on an annual basis.	No exceptions noted.
		Inspected the completed security awareness training for a sample of employees and contractors active within the examination period to verify that employees and contractors were required to complete security awareness training to comply with security policies within the past 12 months.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-013	Employees and contractors are required to complete security awareness training as a component of the onboarding process.	Inquired of the Director of Information Security & Compliance to verify that employees and contractors were required to complete security awareness training as a component of the onboarding process.	No exceptions noted.
		Inspected the acknowledged security awareness trainings for a sample of employees and contractors onboarded within the examination period to verify that employees and contractors were required to complete security awareness training as a component of the onboarding process.	No exceptions noted.
CTL-014	Training courses are made available to new and existing employees to maintain and advance the skill level of personnel.	Inquired of the Director of Information Security & Compliance to verify that training courses were made available to new and existing employees to maintain and advance the skill level of personnel.	No exceptions noted.
		Inspected the dashboard of the online learning portal to verify that training courses were made available to new and existing employees to maintain and advance the skill level of personnel.	No exceptions noted.
CTL-018	Incident response and escalation policies are in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	Inquired of the Director of Information Security & Compliance to verify that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	No exceptions noted.
		Inspected the Incident Response SOP to verify that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	No exceptions noted.
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CTL-019	Information regarding the design and operation of the system and its boundaries is communicated to external users via the company website.	Inquired of the Director of Information Security & Compliance to verify that information regarding the design and operation of the system and its boundaries was communicated to external users via the company website.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the customer guides on the company website to verify that information regarding the design and operation of the system and its boundaries was communicated to external users via the company website.	No exceptions noted.
CTL-020	The entity communicates commitments in customer contracts, master service agreements, marketing materials, or the customer facing website.	Inquired of the Director of Information Security & Compliance to verify that the entity communicated commitments in customer contracts, master service agreements, marketing materials, or the customer facing website.	No exceptions noted.
		Inspected the organization's agreement templates to verify that the entity communicated commitments in customer contracts, master service agreements, marketing materials, or the customer facing website.	No exceptions noted.
Risk Assessment			
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CTL-021	A formal organization strategy and performance policy is in place and updated annually by management to align internal control responsibilities, performance measures and incentives with company business objectives.	Inquired of the Director of Information Security & Compliance to verify that a formal organization strategy and performance policy was in place and updated by management to align internal control responsibilities, performance measures and incentives with company business objectives on an annual basis.	No exceptions noted.
		Inspected the Security Commitment Policy, Fraud Policy, and the Information Security Policy to verify that a formal organization strategy and performance policy was in place and updated by management to align internal control responsibilities, performance measures and incentives with company business objectives within the past 12 months.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-022	The entity has documented relevant operations, reporting, and compliance objectives that are in line with the mission of the organization.	Inquired of the Director of Information Security & Compliance to verify that the entity had documented relevant operations, reporting, and compliance objectives that were in line with the mission of the organization.	No exceptions noted.
		Inspected the Information Security Policy to verify that the entity had documented relevant operations, reporting, and compliance objectives that were in line with the mission of the organization.	No exceptions noted.
CTL-023	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inquired of the Director of Information Security & Compliance to verify that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
		Inspected the risk management standard operating procedures to verify that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CTL-024	Annually, a risk assessment is performed and findings are formally documented for management review.	Inquired of the Director of Information Security & Compliance to verify that a risk assessment was performed and findings were formally documented for management review on an annual basis.	No exceptions noted.
		Inspected the most recent risk assessment to verify that a risk assessment was performed and findings were formally documented for management review within the past 12 months.	No exceptions noted.
CTL-025	The risk assessment includes tolerances for risk by defining acceptable levels and assigning risks to defined levels.	Inquired of the Director of Information Security & Compliance to verify that the risk assessment included tolerances for risk by defining acceptable levels and assigning risks to defined levels.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the risk assessment to verify that the risk assessment included tolerances for risk by defining acceptable levels and assigning risks to defined levels.	No exceptions noted.
CC3.2 - COSO Principle 7: 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.			
CTL-023	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inquired of the Director of Information Security & Compliance to verify that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
		Inspected the risk management standard operating procedures to verify that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CTL-024	Annually, a risk assessment is performed and findings are formally documented for management review.	Inquired of the Director of Information Security & Compliance to verify that a risk assessment was performed and findings were formally documented for management review on an annual basis.	No exceptions noted.
		Inspected the most recent risk assessment to verify that a risk assessment was performed and findings were formally documented for management review within the past 12 months.	No exceptions noted.
CTL-025	The risk assessment includes tolerances for risk by defining acceptable levels and assigning risks to defined levels.	Inquired of the Director of Information Security & Compliance to verify that the risk assessment included tolerances for risk by defining acceptable levels and assigning risks to defined levels.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the risk assessment to verify that the risk assessment included tolerances for risk by defining acceptable levels and assigning risks to defined levels.	No exceptions noted.
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CTL-025	The risk assessment includes tolerances for risk by defining acceptable levels and assigning risks to defined levels.	Inquired of the Director of Information Security & Compliance to verify that the risk assessment included tolerances for risk by defining acceptable levels and assigning risks to defined levels.	No exceptions noted.
		Inspected the risk assessment to verify that the risk assessment included tolerances for risk by defining acceptable levels and assigning risks to defined levels.	No exceptions noted.
CTL-026	Documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process.	Inquired of the Director of Information Security & Compliance to verify that documented policies and procedures were in place to guide personnel in identifying the potential for fraud as part of the risk assessment process.	No exceptions noted.
		Inspected the fraud policy to verify that documented policies and procedures were in place to guide personnel in identifying the potential for fraud as part of the risk assessment process.	No exceptions noted.
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CTL-027	The entity's information technology security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.	Inquired of the Director of Information Security & Compliance to verify that the entity's information technology security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Risk Assessment Tracker and a recent security alert to verify that the entity's information technology security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
CTL-028	The risk assessment process considers significant changes to the internal and external environments.	Inquired of the Director of Information Security & Compliance to verify that the risk assessment process considered significant changes to the internal and external environments.	No exceptions noted.
		Inspected the risk assessment to verify that the risk assessment process considered significant changes to the internal and external environments.	No exceptions noted.
CTL-034	A pre-vetting and due diligence process is performed on potential vendors as a component of the onboarding process.	Inquired of the Director of Information Security & Compliance to verify that a pre-vetting and due diligence process was performed on potential vendors as a component of the onboarding process.	No exceptions noted.
		Inspected the due diligence reviews for the population of vendors onboarded during the examination period to verify that a pre-vetting and due diligence process was performed on potential vendors as a component of the onboarding process.	No exceptions noted.
Monitoring Activities			
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CTL-029	An internal audit program is in place that outlines the methods for monitoring, measurement, scope and frequency, to ensure objectivity.	Inquired of the Director of Information Security & Compliance to verify that an internal audit program was in place that outlined the methods for monitoring, measurement, scope and frequency, to ensure objectivity.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the internal audit standard operating procedures and internal audit Log to verify that an internal audit program was in place that outlined the methods for monitoring, measurement, scope and frequency, to ensure objectivity.	No exceptions noted.
CTL-030	Documented policies and procedures are in place to guide personnel in the performance of the internal audit process.	Inquired of the Director of Information Security & Compliance to verify that documented policies and procedures were in place to guide personnel in the performance of the internal audit process.	No exceptions noted.
		Inspected the internal audit standard operating procedures to verify that documented policies and procedures were in place to guide personnel in the performance of the internal audit process.	No exceptions noted.
CTL-031	Quarterly, vulnerability assessments are performed by security personnel and remediation plans are proposed and tracked through resolution.	Inquired of the Director of Information Security & Compliance to verify that vulnerability assessments were performed by security personnel and remediation plans were proposed and tracked through resolution on a quarterly basis.	No exceptions noted.
		Inspected the vulnerability scan reports and remediation tickets for a sample of quarters to verify that vulnerability assessments were performed by security personnel and remediation plans were proposed and tracked through resolution on a quarterly basis.	No exceptions noted.
CTL-032	Annually, penetration testing is performed by a third party and remediation plans are proposed and tracked through resolution.	Inquired of the Director of Information Security & Compliance to verify that penetration testing was performed by a third party and remediation plans were proposed and tracked through resolution on an annual basis.	No exceptions noted.
		Inspected the penetration test reports to verify that penetration testing was performed by a third party and remediation plans were proposed and tracked through resolution within the past 12 months.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-033	Annually, vendor audit reports are reviewed by management to ensure that third-party providers are in compliance with the organization's requirements.	Inquired of the Director of Information Security & Compliance to verify that vendor audit reports were reviewed by management to ensure that third-party providers were in compliance with the organization's requirements on an annual basis.	No exceptions noted.
		Inspected the most recent third-party service provider audit reports and management's review for a sample of vendors tenured during the examination period to verify that vendor audit reports were reviewed by management to ensure that third-party providers were in compliance with the organization's requirements within the past 12 months.	No exceptions noted.
CC4.2 - COSO Principle 17: 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.			
CTL-027	The entity's information technology security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.	Inquired of the Director of Information Security & Compliance to verify that the entity's information technology security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
		Inspected the Risk Assessment Tracker and a recent security alert to verify that the entity's information technology security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
CTL-035	Assigned risk owners select and develop control activities over technology, documented in the mitigation plans, to mitigate the risks identified during the annual risk assessment process.	Inquired of the Director of Information Security & Compliance to verify that assigned risk owners selected and developed control activities over technology, documented in the mitigation plans, to mitigate the risks identified during the annual risk assessment process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the risk assessment to verify that assigned risk owners selected and developed control activities over technology, documented in the mitigation plans, to mitigate the risks identified during the annual risk assessment process.	No exceptions noted.
CTL-036	Annually, management meets to discuss internal control performance and identified deficiencies to ensure that corrective action is taken.	Inquired of the Director of Information Security & Compliance to verify that management met to discuss internal control performance and identified deficiencies to ensure that corrective action was taken on an annual basis.	No exceptions noted.
		Inspected the most recent meeting minutes to verify that management met to discuss internal control performance and identified deficiencies to ensure that corrective action was taken within the past 12 months.	No exceptions noted.
CTL-037	Quarterly, the Board of Directors meets to discuss internal control performance and identified deficiencies to ensure that corrective action is taken.	Inquired of the Director of Information Security & Compliance to verify that the Board of Directors met on a quarterly basis to discuss internal control performance and identified deficiencies to ensure that corrective action was taken.	No exceptions noted.
		Inspected the meeting invitations for a sample of quarters within the examination period to verify that the Board of Directors met on a quarterly basis to discuss internal control performance and identified deficiencies to ensure that corrective action was taken.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
Control Activities			
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CTL-012	Annually, employees and contractors are required to complete security awareness training to comply with security policies.	Inquired of the Director of Information Security & Compliance to verify that employees and contractors were required to complete security awareness training to comply with security policies on an annual basis.	No exceptions noted.
		Inspected the completed security awareness training for a sample of employees and contractors active within the examination period to verify that employees and contractors were required to complete security awareness training to comply with security policies within the past 12 months.	No exceptions noted.
CTL-013	Employees and contractors are required to complete security awareness training as a component of the onboarding process.	Inquired of the Director of Information Security & Compliance to verify that employees and contractors were required to complete security awareness training as a component of the onboarding process.	No exceptions noted.
		Inspected the acknowledged security awareness trainings for a sample of employees and contractors onboarded within the examination period to verify that employees and contractors were required to complete security awareness training as a component of the onboarding process.	No exceptions noted.
CTL-023	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inquired of the Director of Information Security & Compliance to verify that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the risk management standard operating procedures to verify that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CTL-024	Annually, a risk assessment is performed and findings are formally documented for management review.	Inquired of the Director of Information Security & Compliance to verify that a risk assessment was performed and findings were formally documented for management review on an annual basis.	No exceptions noted.
		Inspected the most recent risk assessment to verify that a risk assessment was performed and findings were formally documented for management review within the past 12 months.	No exceptions noted.
CTL-027	The entity's information technology security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.	Inquired of the Director of Information Security & Compliance to verify that the entity's information technology security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
		Inspected the Risk Assessment Tracker and a recent security alert to verify that the entity's information technology security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
CTL-031	Quarterly, vulnerability assessments are performed by security personnel and remediation plans are proposed and tracked through resolution.	Inquired of the Director of Information Security & Compliance to verify that vulnerability assessments were performed by security personnel and remediation plans were proposed and tracked through resolution on a quarterly basis.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the vulnerability scan reports and remediation tickets for a sample of quarters to verify that vulnerability assessments were performed by security personnel and remediation plans were proposed and tracked through resolution on a quarterly basis.	No exceptions noted.
CTL-032	Annually, penetration testing is performed by a third party and remediation plans are proposed and tracked through resolution.	Inquired of the Director of Information Security & Compliance to verify that penetration testing was performed by a third party and remediation plans were proposed and tracked through resolution on an annual basis.	No exceptions noted.
		Inspected the penetration test reports to verify that penetration testing was performed by a third party and remediation plans were proposed and tracked through resolution within the past 12 months.	No exceptions noted.
CTL-033	Annually, vendor audit reports are reviewed by management to ensure that third-party providers are in compliance with the organization's requirements.	Inquired of the Director of Information Security & Compliance to verify that vendor audit reports were reviewed by management to ensure that third-party providers were in compliance with the organization's requirements on an annual basis.	No exceptions noted.
		Inspected the most recent third-party service provider audit reports and management's review for a sample of vendors tenured during the examination period to verify that vendor audit reports were reviewed by management to ensure that third-party providers were in compliance with the organization's requirements within the past 12 months.	No exceptions noted.
CTL-035	Assigned risk owners select and develop control activities over technology, documented in the mitigation plans, to mitigate the risks identified during the annual risk assessment process.	Inquired of the Director of Information Security & Compliance to verify that assigned risk owners selected and developed control activities over technology, documented in the mitigation plans, to mitigate the risks identified during the annual risk assessment process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the risk assessment to verify that assigned risk owners selected and developed control activities over technology, documented in the mitigation plans, to mitigate the risks identified during the annual risk assessment process.	No exceptions noted.
CTL-042	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	Inquired of the Director of Information Security & Compliance to verify that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
		Inspected the identity and access management configurations to verify that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
CTL-051	Monthly, user access reviews are performed to ensure that access to data is restricted and authorized.	Inquired of the Director of Information Security & Compliance to verify that user access reviews were performed on a monthly basis to ensure that access to data was restricted and authorized.	No exceptions noted.
		Inspected the user access review records for a sample of months within the examination period to verify that user access reviews were performed on a monthly basis to ensure that access to data was restricted and authorized.	No exceptions noted.
CTL-060	A central antivirus server is utilized to manage antivirus software installed on registered workstations and is configured to do the following: -Scan for updates to antivirus definitions and update registered clients on a daily basis -Real time scanning of threats to the system -Monitoring for suspicious activity.	Inquired of the Director of Information Security & Compliance to verify that a central antivirus server was utilized to manage antivirus software installed on registered workstations and was configured to do the following: -Scan for updates to antivirus definitions and update registered clients on a daily basis -Real time scanning of threats to the system -Monitoring for suspicious activity.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the antivirus configurations, documentation, console, update schedule, scan schedule, vulnerability listing, alert configuration, incident listing, and a remediation ticket to verify that a central antivirus server was utilized to manage antivirus software installed on registered workstations and was configured to do the following: -Scan for updates to antivirus definitions and update registered clients on a daily basis -Real time scanning of threats to the system -Monitoring for suspicious activity.	No exceptions noted.
CTL-062	Logging and monitoring applications are configured to collect data from system infrastructure components and used to monitor system performance, potential security threats and vulnerabilities, resource utilization and alert IT personnel upon detection of usual system activity or service requests.	Inquired of the Director of Information Security & Compliance to verify that logging and monitoring applications were configured to collect data from system infrastructure components and used to monitor system performance, potential security threats and vulnerabilities, resource utilization and alert IT personnel upon detection of usual system activity or service requests.	No exceptions noted.
		Inspected the logging and monitoring configurations to verify that logging and monitoring applications were configured to collect data from system infrastructure components and used to monitor system performance, potential security threats and vulnerabilities, resource utilization and alert IT personnel upon detection of usual system activity or service requests.	No exceptions noted.
CTL-076	The ability to implement changes to the production environment is restricted to personnel commensurate with their job role.	Inquired of the Director of Information Security & Compliance to verify that the ability to implement changes to the production environment was restricted to personnel commensurate with their job role.	No exceptions noted.
		Inspected the releasers user listing to verify that the ability to implement changes to the production environment was restricted to personnel commensurate with their job role.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CTL-035	Assigned risk owners select and develop control activities over technology, documented in the mitigation plans, to mitigate the risks identified during the annual risk assessment process.	Inquired of the Director of Information Security & Compliance to verify that assigned risk owners selected and developed control activities over technology, documented in the mitigation plans, to mitigate the risks identified during the annual risk assessment process.	No exceptions noted.
		Inspected the risk assessment to verify that assigned risk owners selected and developed control activities over technology, documented in the mitigation plans, to mitigate the risks identified during the annual risk assessment process.	No exceptions noted.
CTL-042	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	Inquired of the Director of Information Security & Compliance to verify that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
		Inspected the identity and access management configurations to verify that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
CTL-046	Administrative access privileges to the AWS management console are restricted to user accounts accessible by personnel commensurate to their job roles.	Inquired of the Director of Information Security & Compliance to verify that administrative access privileges to the AWS management console were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.
		Inspected the administrator listing to verify that administrative access privileges to the AWS management console were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-047	Administrative access privileges to the GCP management console are restricted to user accounts accessible by personnel commensurate to their job roles.	Inquired of the Director of Information Security & Compliance to verify that administrative access privileges to the GCP management console were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.
		Inspected the administrator listing to verify that administrative access privileges to the GCP management console were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.
CTL-048	Administrative access privileges to the virtual desktop environments are restricted to user accounts accessible by personnel commensurate to their job roles.	Inquired of the Director of Information Security & Compliance to verify that administrative access privileges to the virtual desktop environments were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.
		Inspected the administrator listings to verify that administrative access privileges to the virtual desktop environments were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.
CTL-049	Administrative access privileges to the application are restricted to user accounts accessible by personnel commensurate to their job roles.	Inquired of the Director of Information Security & Compliance to verify that administrative access privileges to the application were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.
		Inspected the administrator listing to verify that administrative access privileges to the application were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.
CTL-054	A firewall system is in place to restrict unauthorized inbound and outbound traffic to and from the network.	Inquired of the Director of Information Security & Compliance to verify that a firewall system was in place to restrict unauthorized inbound and outbound traffic to and from the network.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the firewall policies to verify that a firewall system was in place to restrict unauthorized inbound and outbound traffic to and from the network.	No exceptions noted.
CTL-060	A central antivirus server is utilized to manage antivirus software installed on registered workstations and is configured to do the following: -Scan for updates to antivirus definitions and update registered clients on a daily basis -Real time scanning of threats to the system -Monitoring for suspicious activity.	Inquired of the Director of Information Security & Compliance to verify that a central antivirus server was utilized to manage antivirus software installed on registered workstations and was configured to do the following: -Scan for updates to antivirus definitions and update registered clients on a daily basis -Real time scanning of threats to the system -Monitoring for suspicious activity.	No exceptions noted.
		Inspected the antivirus configurations, documentation, console, update schedule, scan schedule, vulnerability listing, alert configuration, incident listing, and a remediation ticket to verify that a central antivirus server was utilized to manage antivirus software installed on registered workstations and was configured to do the following: -Scan for updates to antivirus definitions and update registered clients on a daily basis -Real time scanning of threats to the system -Monitoring for suspicious activity.	No exceptions noted.
CTL-062	Logging and monitoring applications are configured to collect data from system infrastructure components and used to monitor system performance, potential security threats and vulnerabilities, resource utilization and alert IT personnel upon detection of usual system activity or service requests.	Inquired of the Director of Information Security & Compliance to verify that logging and monitoring applications were configured to collect data from system infrastructure components and used to monitor system performance, potential security threats and vulnerabilities, resource utilization and alert IT personnel upon detection of usual system activity or service requests.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the logging and monitoring configurations to verify that logging and monitoring applications were configured to collect data from system infrastructure components and used to monitor system performance, potential security threats and vulnerabilities, resource utilization and alert IT personnel upon detection of unusual system activity or service requests.	No exceptions noted.
CTL-071	Application changes are tested and documented prior to implementation.	Inquired of the Director of Information Security & Compliance to verify that application changes was tested and documented prior to implementation.	No exceptions noted.
		Inspected the testing completion records for a sample of application changes promoted to production within the examination period to verify that application changes was tested and documented prior to implementation.	No exceptions noted.
CTL-072	Development and test environments are logically separated from the production environment.	Inquired of the Director of Information Security & Compliance to verify that development and test environments were logically separated from the production environment.	No exceptions noted.
		Inspected the separate test and production environments to verify that development and test environments were logically separated from the production environment.	No exceptions noted.
CTL-073	Version control software is utilized to control access to source code and provide version control for application changes.	Inquired of the Director of Information Security & Compliance to verify that version control software was utilized to control access to source code and provide version control for application changes.	No exceptions noted.
		Inspected the version control software to verify that version control software was utilized to control access to source code and provide version control for application changes.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-077	IT personnel review and approve application changes prior to implementation.	Inquired of the Technology Solutions Manager to verify that IT personnel reviewed and approved changes prior to implementation.	No exceptions noted.
		Inspected the change approvals for a sample of application changes promoted to production within the examination period to verify that IT personnel reviewed and approved changes prior to implementation.	No exceptions noted.
CTL-083	The use of MFA is required prior to accessing the virtual desktops.	Inquired of the Director of Information Security & Compliance to verify that the use of MFA was required prior to accessing the virtual desktops.	No exceptions noted.
		Inspected the authentication configurations and a recent logon attempt to verify that the use of MFA was required prior to accessing the virtual desktops.	No exceptions noted.
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CTL-011	Policies and procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	Inquired of the Director of Information Security & Compliance to verify that policies and procedures were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties as outlined in the job description.	No exceptions noted.
		Inspected the Job Requisition and Recruiting SOP to verify that policies and procedures were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties as outlined in the job description.	No exceptions noted.
CTL-016	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.	Inquired of the Director of Information Security & Compliance to verify that policies were documented and maintained that addressed remedial actions for lack of compliance with policies and procedures.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Corrective Action Request Standard Operating Procedures and Code Of Conduct to verify that policies were documented and maintained that addressed remedial actions for lack of compliance with policies and procedures.	No exceptions noted.
CTL-038	Documented policies and procedures are in place to guide personnel with regard to the design, development, implementation, operation, maintenance and monitoring of in-scope systems and are communicated to internal personnel.	Inquired of the Director of Information Security & Compliance to verify that documented policies and procedures were in place to guide personnel with regard to the design, development, implementation, operation, maintenance and monitoring of in-scope systems and were communicated to internal personnel.	No exceptions noted.
		Inspected the software development lifecycle policy, standard operating procedures and the company's intranet to verify that documented policies and procedures were in place to guide personnel with regard to the design, development, implementation, operation, maintenance and monitoring of in-scope systems and were communicated to internal personnel.	No exceptions noted.
CTL-039	An information security policy is formally documented that identifies information required to support the functioning of internal control and achievement of objectives and associated protection, access rights and retention requirements.	Inquired of the Director of Information Security & Compliance to verify that an information security policy was formally documented that identified information required to support the functioning of internal control and achievement of objectives and associated protection, access rights and retention requirements.	No exceptions noted.
		Inspected the Information Security Policy to verify that an information security policy was formally documented that identified information required to support the functioning of internal control and achievement of objectives and associated protection, access rights and retention requirements.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-040	An employee disciplinary policy is in place communicating that an employee may be terminated for noncompliance with a policy and procedure.	Inquired of the Director of Information Security & Compliance to verify that an employee disciplinary policy was in place communicating that an employee may be terminated for noncompliance with a policy and procedure.	No exceptions noted.
		Inspected the Corrective Action Request Standard Operating Procedures and Code Of Conduct to verify that an employee disciplinary policy was in place communicating that an employee may be terminated for noncompliance with a policy and procedure.	No exceptions noted.
Logical and Physical Access Controls			
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.			
CTL-041	AWS is configured to authenticate users with a user account and password and enforce predefined user account and minimum password requirements.	Inquired of the Director of Information Security & Compliance to verify that the AWS was configured to authenticate users with a user account and password and enforce predefined user account and minimum password requirements.	No exceptions noted.
		Inspected the password policy to verify that the AWS was configured to authenticate users with a user account and password and enforce predefined user account and minimum password requirements.	No exceptions noted.
CTL-042	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	Inquired of the Director of Information Security & Compliance to verify that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
		Inspected the identity and access management configurations to verify that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-043	GCP is configured to authenticate users with a user account and password and enforce predefined user account and minimum password requirements.	Inquired of the Director of Information Security & Compliance to verify that the GCP was configured to authenticate users with a user account and password and enforce predefined user account and minimum password requirements.	No exceptions noted.
		Inspected the password policies to verify that the GCP was configured to authenticate users with a user account and password and enforce predefined user account and minimum password requirements.	No exceptions noted.
CTL-044	Language Vault is configured to authenticate users with a user account and password and enforce predefined user account and minimum password requirements.	Inquired of the Director of Information Security & Compliance to verify that the Language Vault was configured to authenticate users with a user account and password and enforce predefined user account and minimum password requirements.	No exceptions noted.
		Inspected the password configurations to verify that the Language Vault was configured to authenticate users with a user account and password and enforce predefined user account and minimum password requirements.	No exceptions noted.
CTL-045	The virtual desktops are configured to authenticate users with a user account and password and enforce predefined user account and minimum password requirements.	Inquired of the Director of Information Security & Compliance to verify that the virtual desktops were configured to authenticate users with a user account and password and enforce predefined user account and minimum password requirements.	No exceptions noted.
		Inspected the Microsoft Azure password policies to verify that the virtual desktops were configured to authenticate users with a user account and password and enforce predefined user account and minimum password requirements.	No exceptions noted.
CTL-046	Administrative access privileges to the AWS management console are restricted to user accounts accessible by personnel commensurate to their job roles.	Inquired of the Director of Information Security & Compliance to verify that administrative access privileges to the AWS management console were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the administrator listing to verify that administrative access privileges to the AWS management console were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.
CTL-047	Administrative access privileges to the GCP management console are restricted to user accounts accessible by personnel commensurate to their job roles.	Inquired of the Director of Information Security & Compliance to verify that administrative access privileges to the GCP management console were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.
		Inspected the administrator listing to verify that administrative access privileges to the GCP management console were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.
CTL-048	Administrative access privileges to the virtual desktop environments are restricted to user accounts accessible by personnel commensurate to their job roles.	Inquired of the Director of Information Security & Compliance to verify that administrative access privileges to the virtual desktop environments were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.
		Inspected the administrator listings to verify that administrative access privileges to the virtual desktop environments were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.
CTL-049	Administrative access privileges to the application are restricted to user accounts accessible by personnel commensurate to their job roles.	Inquired of the Director of Information Security & Compliance to verify that administrative access privileges to the application were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.
		Inspected the administrator listing to verify that administrative access privileges to the application were restricted to user accounts accessible by personnel commensurate to their job roles.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
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.			
CTL-050	System access is revoked upon termination of employment.	Inquired of the Director of Information Security & Compliance to verify that system access was revoked upon termination of employment.	No exceptions noted.
		Inspected the active directory user listing and revoked access confirmations for a sample of users terminated within the examination period to verify that system access was revoked upon termination of employment.	Exceptions noted. 360 Advanced noted that system access was not revoked for two (2) out of the 25 sampled users that were terminated during the examination period.
CTL-051	Monthly, user access reviews are performed to ensure that access to data is restricted and authorized.	Inquired of the Director of Information Security & Compliance to verify that user access reviews were performed on a monthly basis to ensure that access to data was restricted and authorized.	No exceptions noted.
		Inspected the user access review records for a sample of months within the examination period to verify that user access reviews were performed on a monthly basis to ensure that access to data was restricted and authorized.	No exceptions noted.
CTL-080	Logical access requests for employees and contractors are approved by management prior to granting access to system resources and assets.	Inquired of the Director of Information Security & Compliance to verify that logical access requests for employees and contractors was approved by management prior to granting access to system resources and assets.	No exceptions noted.
		Inspected the access requests for a sample of employees and contractors onboarded within the examination period to verify that logical access requests for employees and contractors was approved by management prior to granting access to system resources and assets.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
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.			
CTL-042	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	Inquired of the Director of Information Security & Compliance to verify that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
		Inspected the identity and access management configurations to verify that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
CTL-050	System access is revoked upon termination of employment.	Inquired of the Director of Information Security & Compliance to verify that system access was revoked upon termination of employment.	No exceptions noted.
		Inspected the active directory user listing and revoked access confirmations for a sample of users terminated within the examination period to verify that system access was revoked upon termination of employment.	Exceptions noted. 360 Advanced noted that system access was not revoked for two (2) out of the 25 sampled users that were terminated during the examination period.
CTL-051	Monthly, user access reviews are performed to ensure that access to data is restricted and authorized.	Inquired of the Director of Information Security & Compliance to verify that user access reviews were performed on a monthly basis to ensure that access to data was restricted and authorized.	No exceptions noted.
		Inspected the user access review records for a sample of months within the examination period to verify that user access reviews were performed on a monthly basis to ensure that access to data was restricted and authorized.	No exceptions noted.
CTL-052	Documented policies and procedures are in place to grant access to the systems based on employee job functions.	Inquired of the Director of Information Security & Compliance to verify that documented policies and procedures were in place to grant access to the systems based on employee job functions.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the access control standard operating procedures to verify that documented policies and procedures were in place to grant access to the systems based on employee job functions.	No exceptions noted.
CTL-080	Logical access requests for employees and contractors are approved by management prior to granting access to system resources and assets.	Inquired of the Director of Information Security & Compliance to verify that logical access requests for employees and contractors was approved by management prior to granting access to system resources and assets.	No exceptions noted.
		Inspected the access requests for a sample of employees and contractors onboarded within the examination period to verify that logical access requests for employees and contractors was approved by management prior to granting access to system resources and assets.	No exceptions noted.
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CTL-082	Annually, management obtains and reviews sub-service organization examination reports to ensure controls are suitably designed and operating effectively.	Inquired of the Director of Information Security & Compliance to verify that management obtains and reviews sub-service organization examination reports to ensure controls were suitably designed and operating effectively on an annual basis.	No exceptions noted.
		Inspected the audit report reviews to verify that management obtains and reviews sub-service organization examination reports to ensure controls were suitably designed and operating effectively within the past 12 months.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
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.			
CTL-053	Equipment destruction and disposal procedures are in place to guide personnel in performing sanitization procedures on instances where production data resides to ensure data and software are unrecoverable prior to retiring the virtual asset.	Inquired of the Director of Information Security & Compliance to verify that equipment destruction and disposal procedures were in place to guide personnel in performing sanitization procedures on instances where production data resided to ensure data and software were unrecoverable prior to retiring the virtual asset.	No exceptions noted.
		Inspected the data technology equipment disposal standard operating procedures to verify that equipment destruction and disposal procedures were in place to guide personnel in performing sanitization procedures on instances where production data resided to ensure data and software were unrecoverable prior to retiring the virtual asset.	No exceptions noted.
CTL-082	Annually, management obtains and reviews sub-service organization examination reports to ensure controls are suitably designed and operating effectively.	Inquired of the Director of Information Security & Compliance to verify that management obtains and reviews sub-service organization examination reports to ensure controls were suitably designed and operating effectively on an annual basis.	No exceptions noted.
		Inspected the audit report reviews to verify that management obtains and reviews sub-service organization examination reports to ensure controls were suitably designed and operating effectively within the past 12 months.	No exceptions noted.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CTL-054	A firewall system is in place to restrict unauthorized inbound and outbound traffic to and from the network.	Inquired of the Director of Information Security & Compliance to verify that a firewall system was in place to restrict unauthorized inbound and outbound traffic to and from the network.	No exceptions noted.
		Inspected the firewall policies to verify that a firewall system was in place to restrict unauthorized inbound and outbound traffic to and from the network.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-055	Weekly, security personnel review firewall rulesets.	Inquired of the Director of Information Security & Compliance to verify that security personnel reviewed firewall rulesets on a weekly basis.	No exceptions noted.
		Inspected the weekly security reviews for a sample of weeks within the examination period to verify that security personnel reviewed firewall rulesets on a weekly basis.	No exceptions noted.
CTL-056	Web servers utilize TLS 1.2 or better encryption for web communication sessions.	Inquired of the Director of Information Security & Compliance to verify that web servers utilized TLS 1.2 or better encryption for web communication sessions.	No exceptions noted.
		Inspected the Qualys SSL Report to verify that web servers utilized TLS 1.2 or better encryption for web communication sessions.	No exceptions noted.
CTL-057	An IDS is utilized to analyze and report network events and to report possible network security breaches to IT personnel.	Inquired of the Director of Information Security & Compliance to verify that an IDS was utilized to analyze and report network events and to report possible network security breaches to IT personnel.	No exceptions noted.
		Inspected the alert configurations and a recent alert to verify that an IDS was utilized to analyze and report network events and to report possible network security breaches to IT personnel.	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.			
CTL-032	Annually, penetration testing is performed by a third party and remediation plans are proposed and tracked through resolution.	Inquired of the Director of Information Security & Compliance to verify that penetration testing was performed by a third party and remediation plans were proposed and tracked through resolution on an annual basis.	No exceptions noted.
		Inspected the penetration test reports to verify that penetration testing was performed by a third party and remediation plans were proposed and tracked through resolution within the past 12 months.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-058	Security monitoring tools are configured to alert IT personnel of potential security breaches.	Inquired of the Director of Information Security & Compliance to verify that security monitoring tools were configured to alert IT personnel of potential security breaches.	No exceptions noted.
		Inspected the alert configurations and a recent alert to verify that security monitoring tools were configured to alert IT personnel of potential security breaches.	No exceptions noted.
CTL-059	Documented policies and procedures are in place to guide personnel in the handling and encryption of stored data.	Inquired of the Director of Information Security & Compliance to verify that documented policies and procedures were in place to guide personnel in the handling and encryption of stored data.	No exceptions noted.
		Inspected the data encryption policy and encryption standard operating procedures to verify that documented policies and procedures were in place to guide personnel in the handling and encryption of stored data.	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.			
CTL-060	A central antivirus server is utilized to manage antivirus software installed on registered workstations and is configured to do the following: ➤ Scan for updates to antivirus definitions and update registered clients on a daily basis ➤ Real time scanning of threats to the system ➤ Monitoring for suspicious activity.	Inquired of the Director of Information Security & Compliance to verify that a central antivirus server was utilized to manage antivirus software installed on registered workstations and was configured to do the following: ➤ Scan for updates to antivirus definitions and update registered clients on a daily basis ➤ Real time scanning of threats to the system ➤ Monitoring for suspicious activity.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the antivirus configurations, documentation, console, update schedule, scan schedule, vulnerability listing, alert configuration, incident listing, and a remediation ticket to verify that a central antivirus server was utilized to manage antivirus software installed on registered workstations and was configured to do the following: ➤ Scan for updates to antivirus definitions and update registered clients on a daily basis ➤ Real time scanning of threats to the system ➤ Monitoring for suspicious activity.	No exceptions noted.
System Operations			
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.			
CTL-031	Quarterly, vulnerability assessments are performed by security personnel and remediation plans are proposed and tracked through resolution.	Inquired of the Director of Information Security & Compliance to verify that vulnerability assessments were performed by security personnel and remediation plans were proposed and tracked through resolution on a quarterly basis.	No exceptions noted.
		Inspected the vulnerability scan reports and remediation tickets for a sample of quarters to verify that vulnerability assessments were performed by security personnel and remediation plans were proposed and tracked through resolution on a quarterly basis.	No exceptions noted.
CTL-055	Weekly, security personnel review firewall rulesets.	Inquired of the Director of Information Security & Compliance to verify that security personnel reviewed firewall rulesets on a weekly basis.	No exceptions noted.
		Inspected the weekly security reviews for a sample of weeks within the examination period to verify that security personnel reviewed firewall rulesets on a weekly basis.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-061	Standard build procedures are documented by the IT team for installation and maintenance of production servers and network devices.	Inquired of the Director of Information Security & Compliance to verify that standard build procedures were documented by the IT team for installation and maintenance of production servers and network devices.	No exceptions noted.
		Inspected the Information Security Policy to verify that standard build procedures were documented by the IT team for installation and maintenance of production servers and network devices.	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.			
CTL-018	Incident response and escalation policies are in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	Inquired of the Director of Information Security & Compliance to verify that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	No exceptions noted.
		Inspected the Incident Response SOP to verify that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	No exceptions noted.
CTL-057	An IDS is utilized to analyze and report network events and to report possible network security breaches to IT personnel.	Inquired of the Director of Information Security & Compliance to verify that an IDS was utilized to analyze and report network events and to report possible network security breaches to IT personnel.	No exceptions noted.
		Inspected the alert configurations and a recent alert to verify that an IDS was utilized to analyze and report network events and to report possible network security breaches to IT personnel.	No exceptions noted.
CTL-058	Security monitoring tools are configured to alert IT personnel of potential security breaches.	Inquired of the Director of Information Security & Compliance to verify that security monitoring tools were configured to alert IT personnel of potential security breaches.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the alert configurations and a recent alert to verify that security monitoring tools were configured to alert IT personnel of potential security breaches.	No exceptions noted.
CTL-062	Logging and monitoring applications are configured to collect data from system infrastructure components and used to monitor system performance, potential security threats and vulnerabilities, resource utilization and alert IT personnel upon detection of usual system activity or service requests.	Inquired of the Director of Information Security & Compliance to verify that logging and monitoring applications were configured to collect data from system infrastructure components and used to monitor system performance, potential security threats and vulnerabilities, resource utilization and alert IT personnel upon detection of usual system activity or service requests.	No exceptions noted.
		Inspected the logging and monitoring configurations to verify that logging and monitoring applications were configured to collect data from system infrastructure components and used to monitor system performance, potential security threats and vulnerabilities, resource utilization and alert IT personnel upon detection of usual system activity or service requests.	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.			
CTL-018	Incident response and escalation policies are in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	Inquired of the Director of Information Security & Compliance to verify that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	No exceptions noted.
		Inspected the Incident Response SOP to verify that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	No exceptions noted.
CTL-058	Security monitoring tools are configured to alert IT personnel of potential security breaches.	Inquired of the Director of Information Security & Compliance to verify that security monitoring tools were configured to alert IT personnel of potential security breaches.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the alert configurations and a recent alert to verify that security monitoring tools were configured to alert IT personnel of potential security breaches.	No exceptions noted.
CTL-063	A ticketing system is utilized to document and track incidents and remediation activities.	Inquired of the Director of Information Security & Compliance to verify that a ticketing system was utilized to document and track incidents and remediation activities.	No exceptions noted.
		Inspected the ticketing system to verify that a ticketing system was utilized to document and track incidents and remediation activities.	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.			
CTL-018	Incident response and escalation policies are in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	Inquired of the Director of Information Security & Compliance to verify that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	No exceptions noted.
		Inspected the Incident Response SOP to verify that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	No exceptions noted.
CTL-063	A ticketing system is utilized to document and track incidents and remediation activities.	Inquired of the Director of Information Security & Compliance to verify that a ticketing system was utilized to document and track incidents and remediation activities.	No exceptions noted.
		Inspected the ticketing system to verify that a ticketing system was utilized to document and track incidents and remediation activities.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CTL-018	Incident response and escalation policies are in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	Inquired of the Director of Information Security & Compliance to verify that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	No exceptions noted.
		Inspected the Incident Response SOP to verify that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints.	No exceptions noted.
CTL-064	IT personnel complete incident postmortem reports that include the incident and impact analysis, resolutions, lessons learned and action items.	Inquired of the Director of Information Security & Compliance to verify that IT personnel completed incident postmortem reports that included the incident and impact analysis, resolutions, lessons learned and action items.	No exceptions noted.
		Inspected the completed incident reports for a sample of incidents reported during the examination period to verify that IT personnel completed incident postmortem reports that included the incident and impact analysis, resolutions, lessons learned and action items.	No exceptions noted.
CTL-065	Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by unexpected events.	Inquired of the Director of Information Security & Compliance to verify that disaster recovery and business continuity plans were in place to guide personnel in procedures to protect against disruptions caused by unexpected events.	No exceptions noted.
		Inspected the business continuity and disaster recovery procedure and business contingency plan to verify that disaster recovery and business continuity plans were in place to guide personnel in procedures to protect against disruptions caused by unexpected events.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-066	Annually, disaster recovery plan testing is conducted.	Inquired of the Director of Information Security & Compliance to verify that disaster recovery plan testing was conducted on an annual basis.	No exceptions noted.
		Inspected the most recent disaster recovery test to verify that disaster recovery plan testing was conducted within the past 12 months.	No exceptions noted.
CTL-067	Daily, the automated backup system is configured to perform data backups.	Inquired of the Director of Information Security & Compliance to verify that the automated backup system was configured to perform data backups on a daily basis.	No exceptions noted.
		Inspected the database backup configurations to verify that the automated backup system was configured to perform data backups on a daily basis.	No exceptions noted.
CTL-068	Production data is replicated to a geographically separate data center or availability zone for certain in-scope production systems.	Inquired of the Director of Information Security & Compliance to verify that production data was replicated to a geographically separate data center or availability zone for certain in-scope production systems.	No exceptions noted.
		Inspected the data replication configurations to verify that production data was replicated to a geographically separate data center or availability zone for certain in-scope production systems.	No exceptions noted.
Change Management			
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.			
CTL-069	Documented change management policies and procedures are in place to guide personnel in changes to data management systems and network infrastructure.	Inquired of the Director of Information Security & Compliance to verify that documented change management policies and procedures were in place to guide personnel in changes to data management systems and network infrastructure.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Information Security Policy to verify that documented change management policies and procedures were in place to guide personnel in changes to data management systems and network infrastructure.	No exceptions noted.
CTL-070	A ticketing system is in place to centrally maintain, manage and monitor application changes from development through implementation.	Inquired of the Technology Solutions Manager to verify that a ticketing system was in place to centrally maintain, manage and monitor application changes from development through implementation.	No exceptions noted.
		Inspected the ticketing system exports to verify that a ticketing system was in place to centrally maintain, manage and monitor application changes from development through implementation.	No exceptions noted.
CTL-071	Application changes are tested and documented prior to implementation.	Inquired of the Director of Information Security & Compliance to verify that application changes was tested and documented prior to implementation.	No exceptions noted.
		Inspected the testing completion records for a sample of application changes promoted to production within the examination period to verify that application changes was tested and documented prior to implementation.	No exceptions noted.
CTL-072	Development and test environments are logically separated from the production environment.	Inquired of the Director of Information Security & Compliance to verify that development and test environments were logically separated from the production environment.	No exceptions noted.
		Inspected the separate test and production environments to verify that development and test environments were logically separated from the production environment.	No exceptions noted.
CTL-073	Version control software is utilized to control access to source code and provide version control for application changes.	Inquired of the Director of Information Security & Compliance to verify that version control software was utilized to control access to source code and provide version control for application changes.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the version control software to verify that version control software was utilized to control access to source code and provide version control for application changes.	No exceptions noted.
CTL-074	Administrative access privileges within the version control software are restricted to user accounts accessible by personnel commensurate with their job role.	Inquired of the Director of IT Infrastructure to verify that administrative access privileges within the version control software were restricted to user accounts accessible by personnel commensurate with their job role.	No exceptions noted.
		Inspected the administrator user listing to verify that administrative access privileges within the version control software were restricted to user accounts accessible by personnel commensurate with their job role.	No exceptions noted.
CTL-075	The ability to modify source code libraries within the version control software is restricted to user accounts accessible by personnel commensurate with their job role.	Inquired of the Director of Information Security & Compliance to verify that the ability to modify source code libraries within the version control software was restricted to user accounts accessible by personnel commensurate with their job role.	No exceptions noted.
		Inspected the Bitbucket repository permissions listing to verify that the ability to modify source code libraries within the version control software was restricted to user accounts accessible by personnel commensurate with their job role.	No exceptions noted.
CTL-076	The ability to implement changes to the production environment is restricted to personnel commensurate with their job role.	Inquired of the Director of Information Security & Compliance to verify that the ability to implement changes to the production environment was restricted to personnel commensurate with their job role.	No exceptions noted.
		Inspected the releasers user listing to verify that the ability to implement changes to the production environment was restricted to personnel commensurate with their job role.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-077	IT personnel review and approve application changes prior to implementation.	Inquired of the Technology Solutions Manager to verify that IT personnel reviewed and approved changes prior to implementation.	No exceptions noted.
		Inspected the change approvals for a sample of application changes promoted to production within the examination period to verify that IT personnel reviewed and approved changes prior to implementation.	No exceptions noted.
CTL-081	Infrastructure changes are tested, documented and approved prior to implementation.	Inquired of the Director of Information Security & Compliance to verify that infrastructure changes was tested, documented and approved prior to implementation.	No exceptions noted.
		Inspected the QA testing completion records for a sample of infrastructure changes promoted to production within the examination period to verify that infrastructure changes was tested, documented and approved prior to implementation.	Exception noted. 360 Advanced was unable to obtain a complete and accurate population of infrastructure changes implemented during the examination period.
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CTL-023	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inquired of the Director of Information Security & Compliance to verify that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
		Inspected the risk management standard operating procedures to verify that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-024	Annually, a risk assessment is performed and findings are formally documented for management review.	Inquired of the Director of Information Security & Compliance to verify that a risk assessment was performed and findings were formally documented for management review on an annual basis.	No exceptions noted.
		Inspected the most recent risk assessment to verify that a risk assessment was performed and findings were formally documented for management review within the past 12 months.	No exceptions noted.
CTL-025	The risk assessment includes tolerances for risk by defining acceptable levels and assigning risks to defined levels.	Inquired of the Director of Information Security & Compliance to verify that the risk assessment included tolerances for risk by defining acceptable levels and assigning risks to defined levels.	No exceptions noted.
		Inspected the risk assessment to verify that the risk assessment included tolerances for risk by defining acceptable levels and assigning risks to defined levels.	No exceptions noted.
CTL-034	A pre-vetting and due diligence process is performed on potential vendors as a component of the onboarding process.	Inquired of the Director of Information Security & Compliance to verify that a pre-vetting and due diligence process was performed on potential vendors as a component of the onboarding process.	No exceptions noted.
		Inspected the due diligence reviews for the population of vendors onboarded during the examination period to verify that a pre-vetting and due diligence process was performed on potential vendors as a component of the onboarding process.	No exceptions noted.
CTL-065	Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by unexpected events.	Inquired of the Director of Information Security & Compliance to verify that disaster recovery and business continuity plans were in place to guide personnel in procedures to protect against disruptions caused by unexpected events.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the business continuity and disaster recovery procedure and business contingency plan to verify that disaster recovery and business continuity plans were in place to guide personnel in procedures to protect against disruptions caused by unexpected events.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CTL-033	Annually, vendor audit reports are reviewed by management to ensure that third-party providers are in compliance with the organization's requirements.	Inquired of the Director of Information Security & Compliance to verify that vendor audit reports were reviewed by management to ensure that third-party providers were in compliance with the organization's requirements on an annual basis.	No exceptions noted.
		Inspected the most recent third-party service provider audit reports and management's review for a sample of vendors tenured during the examination period to verify that vendor audit reports were reviewed by management to ensure that third-party providers were in compliance with the organization's requirements within the past 12 months.	No exceptions noted.
CTL-034	A pre-vetting and due diligence process is performed on potential vendors as a component of the onboarding process.	Inquired of the Director of Information Security & Compliance to verify that a pre-vetting and due diligence process was performed on potential vendors as a component of the onboarding process.	No exceptions noted.
		Inspected the due diligence reviews for the population of vendors onboarded during the examination period to verify that a pre-vetting and due diligence process was performed on potential vendors as a component of the onboarding process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-078	Documented policies and procedures are in place to guide personnel in vendor management that addresses risk associated with vendors including, but not limited to, the following: ➤ Specific requirements for a vendor ➤ Due diligence process prior to accepting new vendors ➤ Monitoring process to review vendor compliance on a periodic basis ➤ Termination of contract.	Inquired of the Director of Information Security & Compliance to verify that documented policies and procedures were in place to guide personnel in vendor management that addresses risk associated with vendors including, but not limited to, the following: ➤ Specific requirements for a vendor ➤ Due diligence process prior to accepting new vendors ➤ Monitoring process to review vendor compliance on a periodic basis ➤ Termination of contract.	No exceptions noted.
		Inspected the third party service provider standard operating procedures to verify that documented policies and procedures were in place to guide personnel in vendor management that addresses risk associated with vendors including, but not limited to, the following: ➤ Specific requirements for a vendor ➤ Due diligence process prior to accepting new vendors ➤ Monitoring process to review vendor compliance on a periodic basis ➤ Termination of contract.	No exceptions noted.
CTL-079	The risk assessment includes the analysis of potential threats and vulnerabilities introduced from doing business with vendors and business partners.	Inquired of the Director of Information Security & Compliance to verify that the risk assessment included the analysis of potential threats and vulnerabilities introduced from doing business with vendors and business partners.	No exceptions noted.
		Inspected the risk assessment to verify that the risk assessment included the analysis of potential threats and vulnerabilities introduced from doing business with vendors and business partners.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-082	Annually, management obtains and reviews sub-service organization examination reports to ensure controls are suitably designed and operating effectively.	Inquired of the Director of Information Security & Compliance to verify that management obtains and reviews sub-service organization examination reports to ensure controls were suitably designed and operating effectively on an annual basis.	No exceptions noted.
		Inspected the audit report reviews to verify that management obtains and reviews sub-service organization examination reports to ensure controls were suitably designed and operating effectively within the past 12 months.	No exceptions noted.

SECTION 5:

**INFORMATION PROVIDED BY THE SERVICE ORGANIZATION THAT IS
NOT COVERED BY THE SERVICE AUDITOR'S REPORT**

Management's Responses to the Testing Exceptions

Control #	Control Activities Specified by the Service Organization	Test Applied by the Service Auditor	Testing Results	Management's Response
CTL-002	Annually, employees and contractors are required to acknowledge that the Information Security Policy was received and read.	Inspected the Information Security Policy acknowledgements for a sample of employees and contractors active within the examination period to verify that employees and contractors were required to acknowledge that the Information Security Policy was received and read within the past 12 months.	Exceptions noted. 360 Advanced was unable to verify that the Information Security Policy was received and read for nine (9) out of the 29 employees and contractors selected.	Management has confirmed that the acknowledgment of pending employees will be completed as part of the annual Information Security Refresher. Additionally, we have introduced a new Learning Management Tool to ensure that all employees and contractors review and acknowledge the Information Security Policy during the annual refresher.
CTL-050	System access is revoked upon termination of employment.	Inspected the active directory user listing and revoked access confirmations for a sample of users terminated within the examination period to verify that system access was revoked upon termination of employment.	Exceptions noted. 360 Advanced noted that system access was not revoked for two (2) out of the 25 sampled users that were terminated during the examination period.	Management confirmed that access was disabled at the time of termination, however a formal ticket for access revocation was not created. We have since implemented a new ticketing tool to ensure all terminations are processed through official tickets. Additionally, monthly access reviews are now conducted to ensure timely revocation of access.
CTL-081	Infrastructure changes are tested, documented and approved prior to implementation.	Inspected the QA testing completion records for a sample of infrastructure changes promoted to production within the examination period to verify that infrastructure changes was tested, documented and approved prior to implementation.	Exception noted. 360 Advanced was unable to obtain a complete and accurate population of infrastructure changes implemented during the examination period.	Management confirmed that the changes were carried out in accordance with our Change Management process. However, the activity tickets were not tagged as change tickets. We have now implemented a practice of tagging all tickets based on the specific activity, which will enable more accurate filtering and tracking.

HIPAA Vendor Agreement

This HIPAA Vendor Agreement (“BAA”) is entered into by and between the _____ (“Customer”), and **BIG Language Solutions, LLC**, a Delaware limited liability corporation (“Big Language,” or “Vendor”), effective as of the date last executed below (Effective Date).

Customer and Vendor previously entered or may enter into one or more agreements pursuant to which Vendor provides certain services to Customer (the “Services” and respectively the “Service Agreement”). Together with the Services Agreement, this BAA will govern each party’s respective obligations regarding Protected Health Information (defined below).

The parties hereby agree as follows:

1. Definitions

- a. “Breach” has the definition given to it under HIPAA.
- b. “Covered Entity” has the definition given to it under HIPAA.
- c. “Covered Services” means any portion or aspect of the Services in or through which PHI is stored or processed under the Service Agreement.
- d. “Designated Record Set” has the definition give to it under HIPAA.
- e. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996 and the rules and the regulations thereunder, as amended.
- f. “HITECH Act” means the Health Information Technology for Economic and Clinical Health Act enacted in the United States Congress, which is Title XIII of the American Recovery & Reinvestment Act, and the regulations thereunder, as amended.
- g. “Protected Health Information” or “PHI” has the definition given to it under HIPAA and for purposes of this BAA is limited to PHI within data made available by Customer to Vendor and that Vendor accesses through the Covered Services in connection with Customer’s permitted use of Covered Services.
- h. “Required by Law” has the definition given to it under HIPAA.
- i. “Security Incident” has the definition given to it under HIPAA.
- j. “Subcontractor” has the definition given to it under HIPAA.

Any other capitalized terms used and not defined in this BAA are as defined within HIPAA.

2. Applicability

This BAA applies to the extent Customer is acting as a Covered Entity or a Business Associate to create, receive, maintain, or transmit PHI via a Covered Service and to the extent Vendor, as a result, is deemed under HIPAA to be acting as a Business Associate or Subcontractor of Customer. Customer acknowledges that this BAA does not apply to (a) any other Vendor product, service, or feature that is not a Covered Service; or (b) any PHI that Customer creates, receives, maintains, or transmits outside of the Covered Services (including Customer’s use of its offline or on-premise storage tools or third-party applications).

3. Permitted Use and Disclosure of PHI

- Except as otherwise stated in this BAA, Vendor may use and disclose PHI only (i) as permitted or required by the Services Agreements and/or this BAA or (ii) as Required by Law.
- Vendor may use and disclose PHI for its proper management and administration and to carry out its legal responsibilities, provided that any disclosure of PHI for such purposes may only occur if (i) Required by Law; or (ii) Vendor obtains written reasonable assurances from the person to whom PHI will be disclosed that it will be held in confidence, used only for the purpose for which it was disclosed, and that Vendor will be notified of any Breach or Security Incident.

4. Customer Obligations.

- Customer will not request that Vendor or the Covered Services use or disclose PHI in any manner that would not be permissible under HIPAA if done by Customer (if Customer is a Covered Entity) or by the Covered Entity to which Customer is a Business Associate (unless expressly permitted under HIPAA for a Business Associate).
- For End Users that use the Covered Services in connection with PHI, Customer will use any controls that Vendor may make available within the Services, to ensure its use of PHI is limited to the Covered Services. Customer acknowledges and agrees that Customer is solely responsible for ensuring that its and its end users' and customers' use of the Covered Services (to the extent applicable) complies with HIPAA and HITECH

5. Appropriate Safeguards

Vendor and Customer will each use appropriate safeguards designed to prevent against unauthorized use or disclosure of PHI, and as otherwise required under HIPAA, with respect to the Covered Services.

6. Reporting and Related Obligations.

- Vendor will promptly notify Customer of (i) any Security Incident of which Vendor becomes aware; and (ii) any Breach that Vendor discovers, provided that any notice for Breach will be made promptly and without unreasonable delay, and in no case later than 60 calendar days after discovery. Notifications made under this section will describe, to the extent possible, details of a Breach, including steps taken to mitigate the potential risks and steps Vendor recommends Customer take to address the Breach.
- Vendor will send any applicable notifications to the notification email address provided by Customer to Vendor or via another direct communication with Customer.

7. Subcontractors

Vendor will take appropriate measures to ensure that any Subcontractors used by Vendor to perform its obligations under the Services Agreements that require access to PHI on behalf of Vendor are bound by written obligations that provide the same material level of protection for PHI as this BAA. To the extent Vendor uses Subcontractors in its performance of obligations hereunder, Vendor will remain responsible for their performance as if performed by Vendor.

8. Access and Amendment.

Customer acknowledges and agrees that Customer is solely responsible for the form and content of PHI maintained by Customer within the Covered Services, including whether Customer maintains such PHI in a Designated Record Set within the Covered Services. Vendor will provide Customer with access to Customer's PHI via the Covered Services or as otherwise agreed by the parties from time to time so that Customer may fulfill its obligations under HIPAA with respect to Individuals' rights of access and amendment, but will have no other obligations to Customer or any Individual with respect to the rights afforded to Individuals by HIPAA with respect to Designated Record Sets, including rights of access or amendment of PHI. Customer is responsible for managing its use of the Covered Services and PHI to appropriately respond to such individual requests.

9. Accounting of Disclosures.

Vendor will document disclosures of PHI by Vendor and provide an accounting of such disclosures to Customer as and to the extent required of a Business Associate under HIPAA and in accordance with the requirements applicable to a Business Associate under HIPAA.

10. Access to Records

To the extent required by law, and subject to all applicable legal privileges, Vendor will make its internal practices, books, and records concerning the use and disclosure of PHI received from Customer, or created

or received by Vendor on behalf of Customer, available to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for the purpose of the Secretary determining compliance with this BAA.

11. Expiration and Termination.

- This BAA will terminate on the earlier of (i) a permitted termination in accordance with Section 11(b), or (ii) the expiration or termination of all Services Agreements under which Customer has access to a Covered Service.
- If either party materially breaches this BAA, the other party may terminate this BAA on 10 days' written notice to the breaching party unless the breach is cured within the 10-day period. If a cure under this Section 11(b) is not reasonably possible, either party may immediately terminate this BAA, or if neither termination nor cure is reasonably possible under this Section 11(b), either party may report the violation to the Secretary, subject to all applicable legal privileges.
- If this BAA is terminated earlier than all Services Agreements and the parties do not enter into a similar agreement to replace this BAA, Customer may continue to use the Services in accordance with the Services Agreements, but must delete any PHI it maintains in the Covered Services and cease to further create, receive, maintain, or transmit such PHI to Vendor.

12. Return/Destruction of Information

Upon termination or expiration of all Services Agreements, Vendor will return or destroy all PHI received from Customer, or created or received by Vendor on behalf of Customer; provided, however, that if such return or destruction is not feasible, Vendor will extend the protections of this BAA to the PHI not returned or destroyed and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.

13. Miscellaneous.

- Sections 12 (Return/Destruction of Information) and 13 (Miscellaneous) will survive termination or expiration of this BAA.
- This BAA is subject to the Service Agreement, including any provisions in the Service Agreement relating to rights, obligations, indemnification coverage and/or liability coverage and limitations of each party. Except as expressly provided under this BAA, the terms of the Services Agreement(s) remain in full force and effect.

The Parties agree to the above terms and have executed this Agreement as of the date(s) set forth below.

CUSTOMER: _____

BIG LANGUAGE SOLUTIONS, LLC

By (Signature): _____

By (Signature): _____

Name (Printed): _____

Name (Printed): _____

Title: _____

Title: _____

Date: _____

Date: _____

List of languages for Document Translation

Sr. No.	Languages	Availability
1	Acholi	Yes
2	Afar	Yes
3	Afrikaans	Yes
4	Albanian	Yes
5	Amharic	Yes
6	Arabic	Yes
7	Armenian	Yes
8	Assamese	Yes
9	Azerbaijani	Yes
10	Balochi	Yes
11	Bambara	Yes
12	Basque	Yes
13	Belarusian	Yes
14	Bengali	Yes
15	Berber	Yes
16	Bhojpuri	Yes
17	Bosnian	Yes
18	Bulgarian	Yes
19	Burmese	Yes
	Cantonese	Yes
20	Catalan	Yes
21	Cebuano	Yes
22	Chaldean	Yes
23	Chamorro	Yes
24	Chinese (Simplified)	Yes
25	Chinese (Traditional)	Yes
26	Chuukese	Yes
27	Croatian	Yes
28	Czech	Yes
29	Dakota	Yes
30	Danish	Yes
31	Dari	Yes
32	Dutch	Yes
33	Dzongkha	Yes
34	Edo	Yes
35	English	Yes

36	Estonian	Yes
37	Ewe	Yes
38	Fante	Yes
39	Fijian	Yes
40	Finnish	Yes
41	Flemish	Yes
42	French	Yes
43	Frisian	Yes
44	Fulah (Fula, Fulani)	Yes
45	Gaelic (Irish/Scottish)	Yes
46	Georgian	Yes
47	German	Yes
48	Greek	Yes
49	Gujarati	Yes
50	Haitian Creole	Yes
51	Hakka	Yes
52	Hausa	Yes
53	Hebrew	Yes
54	Hiligaynon	Yes
55	Hindi	Yes
56	Hmong	Yes
57	Hungarian	Yes
58	Icelandic	Yes
59	Igbo	Yes
60	Ilocano	Yes
61	Indonesian	Yes
62	Italian	Yes
63	Iu Mien	Yes
64	Javanese	Yes
65	Japanese	Yes
66	Kannada	Yes
67	Kashmiri	Yes
68	Kazakh	Yes
69	Khmer (Cambodian)	Yes
70	K'iche'	Yes
71	Kikuyu	Yes
72	Kinyarwanda	Yes
73	Kirundi	Yes
74	Korean	Yes
75	Kpelle	Yes
76	Krio (Sierra Leone)	Yes

77	Kurdish	Yes
78	Kyrgyz	Yes
79	Lao	Yes
80	Latin	Yes
81	Latvian	Yes
82	Lingala	Yes
83	Lithuanian	Yes
84	Luganda	Yes
85	Luxembourgish	Yes
86	Macedonian	Yes
87	Malagasy	Yes
88	Malay	Yes
89	Malayalam	Yes
90	Maltese	Yes
	Mandarin	Yes
91	Mandinka	Yes
92	Maori	Yes
93	Marathi	Yes
94	Marshallese	Yes
95	Mongolian	Yes
96	Montenegrin	Yes
97	Nepali	Yes
98	Norwegian	Yes
99	Nuer	Yes
100	Oromo	Yes
101	Palauan	Yes
102	Pashto	Yes
103	Polish	Yes
104	Portuguese	Yes
105	Punjabi	Yes
106	Quechua	Yes
107	Romanian	Yes
108	Russian	Yes
109	Samoan	Yes
110	Sango	Yes
111	Saraiki	Yes
112	Serbian	Yes
113	Shona	Yes
114	Sindhi	Yes
115	Sinhalese	Yes
116	Slovak	Yes

117	Slovene	Yes
118	Somali	Yes
119	Sotho	Yes
120	Spanish	Yes
121	Swahili	Yes
122	Swedish	Yes
123	Sylheti	Yes
124	Tagalog	Yes
125	Tajik	Yes
126	Tamil	Yes
127	Tatar	Yes
128	Telugu	Yes
129	Tetum	Yes
130	Thai	Yes
131	Tibetan	Yes
132	Tigre	Yes
133	Tigrinya	Yes
134	Tok Pisin	Yes
135	Tongan	Yes
136	Tswana	Yes
137	Turkish	Yes
138	Turkmen	Yes
139	Twi	Yes
140	Uighur	Yes
141	Ukrainian	Yes
142	Urdu	Yes
143	Uzbek	Yes
144	Vietnamese	Yes
145	Welsh	Yes
146	Wolof	Yes
147	Xhosa	Yes
148	Yao	Yes
149	Yiddish	Yes
150	Yoruba	Yes
151	Zulu	Yes

List of languages for On-Demand OPI

Sr. No.	Languages	Availability
1	Akan	Yes
2	Albanian	Yes
3	Amharic	Yes
4	Arabic	Yes
5	Armenian	Yes
6	Bengali	Yes
7	Bosnian	Yes
8	Bulgarian	Yes
9	Burmese	Yes
10	Cambodian (Khmer)	Yes
11	Cantonese	Yes
12	Cape Verde Creole	Yes
13	Chinese	Yes
14	Chin-Falam	Yes
15	Chin-Hahka	Yes
16	Chin-Mizo	Yes
17	Chuukese (Trukese)	Yes
18	Croatian	Yes
19	Czech	Yes
20	Dari	Yes
21	Dinka	Yes
22	Farsi (Persian)	Yes
23	Farsi-Tajik	Yes
24	Filipino	Yes
25	French	Yes
26	French Creole	Yes
27	French-Canadian	Yes
28	Georgian	Yes
29	German	Yes
30	Gujarati	Yes
31	Haitian Creole	Yes
32	Hebrew	Yes
33	Hindi	Yes
34	Hmong	Yes
35	Hungarian	Yes
36	Ibo (Igbo)	Yes

37	Indonesian	Yes
38	Italian	Yes
39	Japanese	Yes
40	Kaqchikel	Yes
41	Karen	Yes
42	K'iche' (Quiche)	Yes
43	Kikuyu (Gikuyu)	Yes
44	Kinyarwanda	Yes
45	Kirundi (Rundi)	Yes
46	Korean	Yes
47	Kurdish	Yes
48	Kurdish-Sorani	Yes
49	Laotian	Yes
50	Lingala	Yes
51	MaayMaay	Yes
52	Malay (Bahasa Melayu)	Yes
53	Malayalam	Yes
54	Mam	Yes
55	Mandarin	Yes
56	Marshallese	Yes
57	Mixteco Bajo	Yes
58	Moldavian	Yes
59	Mongolian	Yes
60	Montenegrin	Yes
61	Nepali	Yes
62	Oromo (Oromifa)	Yes
63	Pashto	Yes
64	Polish	Yes
65	Portuguese	Yes
66	Portuguese-Brazilian	Yes
67	Pulaar	Yes
68	Punjabi	Yes
69	Rohingya	Yes
70	Romanian	Yes
71	Russian	Yes
72	Serbian	Yes
73	Serbo Croatian	Yes
74	Sichuanese	Yes
75	Slovak	Yes
76	Somali	Yes

77	Spanish	Yes
78	Sudanese	Yes
79	Swahili	Yes
80	Sylheti	Yes
81	Tagalog	Yes
82	Tamil	Yes
83	Telugu	Yes
84	Thai	Yes
85	Tigrinya	Yes
86	Turkish	Yes
87	TWI	Yes
88	Ukrainian	Yes
89	Urdu	Yes
90	Uzbek	Yes
91	Vietnamese	Yes
92	Visayan-Cebuano	Yes
93	Wolof	Yes
94	Yoruba	Yes
95	Zapoteco	Yes

List of languages for On-Demand VRI

Sr. No.	Languages	Availability
1	American Sign Language (ASL)	Yes
2	Amharic	Yes
3	Arabic	Yes
4	Bengali	Yes
5	Burmese	Yes
6	Cantonese	Yes
7	French	Yes
8	Gujarati	Yes
9	Hindi	Yes
10	Japanese	Yes
11	Korean	Yes
12	Mandarin	Yes
13	Nepali	Yes
14	Pashto	Yes
15	Polish	Yes
16	Portuguese	Yes
17	Punjabi	Yes
18	Russian	Yes
19	Spanish	Yes
20	Tagalog	Yes
21	Vietnamese	Yes

List of languages for Live Voice

Sr. No.	Languages	Availability
1	Albanian	Yes
2	American Sign Language (ASL)	Yes
3	Arabic	Yes
4	Armenian	Yes
5	Bengali	Yes
6	Burmese	Yes
7	Cambodian	Yes
8	Cantonese	Yes
9	Dari	Yes
10	Farsi	Yes
11	French	Yes
12	French Canadian	Yes
13	German	Yes
14	Gujarati	Yes
15	Hassaniya	Yes
16	Hindi	Yes
17	Hmong	Yes
18	Italian	Yes
19	Japanese	Yes
20	Korean	Yes
21	Laotian	Yes
22	Lebanese	Yes
23	Mandarin	Yes
24	Nepali	Yes
25	Polish	Yes
26	Portuguese	Yes
27	Punjabi	Yes
28	Romanian	Yes
29	Russian	Yes
30	Somali	Yes
31	Spanish	Yes
32	Tagalog	Yes
33	Thai	Yes
34	Ukrainian	Yes
35	Vietnamese	Yes